Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/1382

18.7.2025.

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2025/1382

(2025. gada 15. jūlijs),

kas pieņemts, ievērojot Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu pietiekamu aizsardzību Eiropas Patentu organizācijā

(izziņots ar dokumenta numuru C(2025) 4626)

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) ([1]), un jo īpaši tās 45. panta 3. punktu,

tā kā:

1. IEVADS

(1) Ar Regulu (ES) 2016/679 ir paredzēti noteikumi, saskaņā ar kuriem pārziņi vai apstrādātāji Savienībā var pārsūtīt personas datus trešām valstīm un starptautiskām organizācijām, ciktāl šāda nosūtīšana ietilpst regulas piemērošanas jomā. Noteikumi par datu starptautisko pārsūtīšanu ir izklāstīti minētās regulas V nodaļā (44.–50. pants). Lai gan personas datu plūsma uz valstīm un starptautiskām organizācijām ārpus Eiropas Savienības un no tām ir būtiska pārrobežu tirdzniecības un starptautiskās sadarbības paplašināšanas nodrošināšanai, datu pārsūtīšana uz trešām valstīm un starptautiskām organizācijām nedrīkst samazināt Savienībā nodrošināto personas datu aizsardzības līmeni ([2]).

(2) Atbilstoši Regulas (ES) 2016/679 45. panta 3. punktam Komisija ar īstenošanas aktu var nolemt, ka trešā valsts, trešās valsts teritorija vai viens vai vairāki konkrēti sektori, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni. Saskaņā ar šo nosacījumu personas datus var pārsūtīt starptautiskai organizācijai bez nepieciešamības saņemt jebkādu papildu atļauju, kā paredzēts Regulas (ES) 2016/679 45. panta 1. punktā un izklāstīts 103. apsvērumā.

(3) Kā norādīts Regulas (ES) 2016/679 45. panta 2. punktā, lēmums par aizsardzības līmeņa pietiekamību jāpieņem, pamatojoties uz visaptverošu starptautiskā organizācijas tiesību režīma analīzi, gan attiecībā uz noteikumiem, kas piemērojami datu saņēmējiem, gan attiecībā uz ierobežojumiem un aizsardzības pasākumiem saistībā ar publisko iestāžu piekļuvi personas datiem. Komisijai novērtējumā jānosaka, vai attiecīgā starptautiskā organizācija garantē aizsardzības līmeni, kurš "pēc būtības ir līdzvērtīgs" Savienībā nodrošinātajam ([3]). Standarts, pēc kura tiek novērtēta "līdzvērtība pēc būtības", ir paredzēts Savienības tiesību aktos, jo īpaši Regulā (ES) 2016/679, kā arī Eiropas Savienības Tiesas judikatūrā ([4]). Lai sīkāk precizētu šo standartu un sniegtu norādījumus šajā sakarā, nozīme ir arī Eiropas Datu aizsardzības kolēģijas (EDAK) "pietiekamības atsaucēm" ([5]).

([1]) OV L 119, 4.5.2016, 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Sk. Regulas (ES) 2016/679.101. apsvērumu.
([3]) Sk. Regulas (ES) 2016/679.104. apsvērumu.
([4]) Sk. spriedumu lietā C-311/18 *Facebook Ireland* un *Schrems* ("Schrems II"), ECLI:EU:C:2020:559, 94. punkts.
([5]) Eiropas Datu aizsardzības kolēģija, Pietiekamības atsauces, *WP 254 rev. 01*, pieejamas https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Kā precizējusi Tiesa, trešai valstij vai starptautiskai organizācijai nevar prasīt nodrošināt tādu aizsardzības līmeni, kas ir identisks Savienības tiesību sistēmā garantētajam ([6]). Proti, attiecīgās trešās valsts vai starptautiskās organizācijas izmantotie līdzekļi personas datu aizsardzībai var atšķirties no Savienībā izmantotajiem, ja vien tie praksē efektīvi nodrošina pietiekamu aizsardzības līmeni ([7]). Tāpēc aizsardzības līmeņa pietiekamības standarts neparedz Savienības noteikumu precīzu replicēšanu. Drīzāk ir jāpārbauda, vai, izmantojot privātuma tiesību un datu aizsardzības pasākumu būtību (tostarp to efektīvu īstenošanu, uzraudzību un izpildi), kā arī personas datu pārsūtīšanas apstākļus, ārvalstu sistēma kopumā nodrošina vajadzīgo aizsardzības līmeni ([8]).

(5) Komisija ir izanalizējusi Eiropas Patentu organizācijas tiesisko regulējumu un praksi. Pamatojoties uz 7.–100. apsvērumā izklāstītajiem konstatējumiem, Komisija secina, ka personas datiem, kas tiek pārsūtīti no Savienības uz Eiropas Patentu organizāciju Regulas (ES) 2016/679 piemērošanas jomas ietvaros, EPO nodrošina pietiekamu aizsardzības līmeni.

(6) Saskaņā ar šo lēmumu datu pārsūtīšanai no pārziņiem un apstrādātājiem Savienībā uz Eiropas Patentu organizāciju nav nepieciešams saņemt nekādu papildu atļauju. Šim lēmumam nebūtu jāietekmē Regulas (ES) 2016/679 tieša piemērošana vienībām, kur ir izpildīti minētās regulas 3. pantā paredzētie nosacījumi attiecībā uz tās teritoriālo darbības jomu.

2. PERSONAS DATU APSTRĀDEI PIEMĒROJAMIE NOTEIKUMI

2.1. Eiropas Patentu organizācijas struktūra un uzdevumi

(7) Eiropas Patentu organizācija ir starpvaldību organizācija, kas izveidota 1977. gada 7. oktobrī, pamatojoties uz Eiropas Patentu konvenciju (EPK). Organizācijas mītne ir Minhenē, un tajā ir 39 līgumslēdzējas valstis, proti, visas Savienības dalībvalstis, Islande, Norvēģija un Lihtenšteina, kā arī Albānija, Ziemeļmaķedonija, Monako, Sanmarīno, Serbija, Šveice, Melnkalne, Apvienotā Karaliste un Turcija ([9]).

(8) Organizācijai ir juridiskas personas statuss ([10]), un tā sastāv no divām struktūrām ([11]): Eiropas Patentu iestādes ("Iestāde") un Administratīvās padomes. EPO galvenais uzdevums ir saskaņā ar EPK piešķirt Eiropas patentus ([12]), ko Administratīvās padomes uzraudzībā veic Iestāde. Administratīvo padomi veido līgumslēdzēju valstu pārstāvji, un tā īsteno likumdošanas pilnvaras EPO vārdā. Tā arī atbild par politikas jautājumiem un uzrauga Iestādes darbību ([13]). Iestādes, kas darbojas kā EPO izpildstruktūra, vadītājs ir priekšsēdētājs ([14]), kurš vada Iestādi (Priekšsēdētājs) un atskaitās Administratīvajai padomei ([15]). Priekšsēdētājs tostarp sagatavo un īsteno Iestādes budžetu, ieceļ un uzrauga Iestādes personālu, īsteno disciplināras pilnvaras attiecībā uz darbiniekiem, nodrošina Iestādes darbību, ieskaitot iekšēju administratīvu norādījumu pieņemšanu un sabiedrības informēšanu, un var iesniegt Administratīvajai padomei priekšlikumus par grozījumiem Konvencijā, vispārējos noteikumos vai lēmumos, kas ir tās kompetencē ([16]).

([6]) Spriedums lietā C-362/14 *Schrems* ("*Schrems* I"), ECLI:EU:C:2015:650, 73. punkts.
([7]) *Schrems* I, 74. punkts.
([8]) *Schrems* I, 75. punkts.
([9]) Līgumslēdzēju valstu skaits 2025. gada februārī.
([10]) EPK 5. panta 1. punkts.
([11]) EPK 4. panta 2. punkts.
([12]) Katrā līgumslēdzējā valstī, attiecībā uz kuru Eiropas patents ir piešķirts, tas principā darbojas tāpat kā šīs valsts piešķirts patents (sk. EPK 2. panta 2. punktu).
([13]) EPK 26. un 33. pants.
([14]) Priekšsēdētāju ieceļ Administratīvā padome, un viņš ārēji pārstāv EPO (EPK 5. panta 3. punkts).
([15]) EPK 10. panta 1. punkts.
([16]) EPK 10. panta 2. punkts.

Iestāde sastāv no dažādām nodaļām, tostarp pieņemšanas nodaļas, juridiskās nodaļas, pārbaudes un iebildumu nodaļas un apelācijas padomes (iekšēja neatkarīga struktūra, kurā var pārsūdzēt lēmumus, ko EPO pieņēmusi patentu piešķiršanas procesā) ([17]).

(9) Pildot savus uzdevumus, EPO saņem personas datus no vairākiem dažādiem dalībniekiem Savienībā. Patentu pieteicēji EPO pastāvīgi iesniedz Eiropas patentu pieteikumus ([18]), vai arī EPO tos nosūta dalībvalstu patentu biroji ([19]). EPO arī saņem un apstrādā personas datus saistībā ar uzdevumiem, kas tai uzticēti saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1257/2012 ([20]). Šie uzdevumi ietver Eiropas patentu vienota spēka pieprasījumu saņemšanu un izskatīšanu, ikgadējo maksu iekasēšanu un vienota spēka reģistrēšanu ([21]). Šajā kontekstā EPO no Vienotās patentu tiesas (VPT) saņem arī pieprasījumus par Iestādes apelācijas padomē iesniegtajām pārsūdzībām ([22]), kuri var ietvert attiecīgās lietas identificēšanai nepieciešamos personas datus ([23]).

(10) Tāpat EPO saņem personas datus, kas ietverti starptautiskajos patentu pieteikumos, kad tā rīkojas saskaņā ar Nolīgumu par sadarbību patentu jomā (*PCT*), kas ir starptautisks līgums, kurš ļauj pieteikuma iesniedzējiem iegūt patentus, kas ir spēkā visās *PCT* līgumslēdzējās valstīs ([24]). EPO darbojas kā starptautiska meklēšanas iestāde saskaņā ar *PCT* un šajā statusā pārskata starptautiskos pieteikumos atklāto izgudrojumu patentspēju, kas palīdz pieteikuma iesniedzējiem noteikt, vai iesniegt pieteikumu izskatīšanai pēc būtības valsts/Savienības līmenī ([25]).

(11) EPO cieši sadarbojas arī ar valstu patentu birojiem visās dalībvalstīs "Eiropas Patentu tīkla" kontekstā un šajā sakarā apmainās ar personas datiem ar tiem, piemēram, nodrošinot apmācības kursus un IT pakalpojumus, lai atbalstītu un stiprinātu sadarbību EPK ietvaros. Tāpat tā ir noslēgusi divpusējus sadarbības nolīgumus ar dalībvalstīm, kas ietver personas datu apmaiņu, piemēram, saistībā ar darba grupu izveidi, tehnisko ekspertu norīkošanu un nosūtīšanu utt. Tā arī cieši sadarbojas ar Eiropas Savienības Intelektuālā īpašuma biroju (*EUIPO*), piemēram, rīkojot kopīgus apmācības kursus un izpratnes veicināšanas pasākumus, kā arī norīkojot ekspertus.

([17]) Apelācijas padomju locekļus ieceļ Administratīvā padome (pēc Priekšsēdētāja priekšlikuma), un tie darbojas neatkarīgi (EPK 11. panta 3. punkts un 23. pants).

([18]) Tie ietver, piemēram, pieteikuma iesniedzēju vārdu/nosaukumu, adresi, valstspiederību un tālruņa numuru; izgudrotāju un patentu pārstāvju vārdu/nosaukumu un adresi; personas, kura veic maksājumus, vārdu/nosaukumu un finanšu informāciju u. c. EPO var iegūt papildu personas datus, ja trešā persona iebilst pret patenta piešķiršanu, un tādā gadījumā EPO rīcībā var nonākt papildu informācija, piemēram, trešo personu apsvērumi, pierādījumi un rakstiski paziņojumi, (sk. EPK īstenošanas noteikumus, piemēram, 41. panta 2. punktu, 143. panta 1. punkta h) apakšpunktu, 92. panta 2. punkta c) apakšpunktu, 19. panta 1. punktu, 53. panta 1. punktu utt.). Sk. arī 9. pantu Priekšsēdētāja lēmumā par patentu piešķiršanas procedūru.

([19]) Eiropas patenta pieteikumu var iesniegt līgumslēdzējas valsts centrālajā rūpnieciskā īpašuma birojā vai citā kompetentā iestādē. Valsts iestāde pārbauda pieteikumu saskaņā ar drošības vai citām valsts prasībām un tad to pārsūta EPO.

([20]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1257/2012 (2012. gada 17. decembris), ar ko īsteno ciešāku sadarbību attiecībā uz vienotas patentaizsardzības izveidi (OV L 361, 31.12.2012., 1. lpp., ELI: http://data.europa.eu/eli/reg/2012/1257/oj).

([21]) Vienotie patenti, kuriem ir vienots spēks visās iesaistītajās dalībvalstīs, tiek centralizēti reģistrēti EPO, neveicot turpmākus administratīvus pasākumus valsts līmenī (kā tas ir nepieciešams Eiropas patentiem).

([22]) 2024. gada decembrī EPI pieņēma noteikumus par neatkarīgu pārraudzības mehānismu attiecībā uz personas datu apstrādi, ko apelācijas padome veic, pildot tiesas funkcijas. Pieejams šeit: https://www.epo.org/en/about-us/transparency-portal?search_description=CA%2FD+19%2F24&op=&sort_by=most&items_per_page=10.

([23]) Vienotā patentu tiesa ir izveidota, pamatojoties uz Vienotās patentu tiesas izveides nolīgumu (OV C 175, 20.6.2013., 1. lpp.), un tai ir izņēmuma jurisdikcija *inter alia* attiecībā uz Eiropas patentiem (tiek piemērots pārejas periods) un vienota spēka Eiropas patentiem (piemēram, attiecībā uz prasībām par faktiskiem vai draudošiem pārkāpumiem un ar tām saistītiem aizsardzības pasākumiem, prasībām par pārkāpuma neesamības konstatēšanu, prasībām par pagaidu un aizsardzības pasākumiem un aizliegumiem, atcelšanas prasībām un pretprasībām par atcelšanu). VPT ir arī ekskluzīva jurisdikcija attiecībā uz EPO lēmumiem, kad tā veic savus uzdevumus vienotās patentu aizsardzības jomā.

([24]) Pārskatu par *PCT* procedūru sk. *PCT Applicant's Guide – Introduction to the International Phase*, kas pieejams tīmekļa vietnē https://www.wipo.int/pct/en/guide/index.html, jo īpaši 3. nodaļā, un *Guide for applicants: PCT procedure before the EPO (Euro-PCT Guide)*, 16. izdevums, 2023. g. 1 janvāris, pieejams šeit https://www.epo.org/en/legal/guide-europct/2023/index.html. Attiecībā uz personas datu kategorijām, ko Eiropas Patentu iestāde apstrādā saistībā ar tiesvedību saskaņā ar *PCT*, skat. jo īpaši Eiropas Patentu iestādes Priekšsēdētāja 2021. gada 13. decembra lēmuma par personas datu apstrādi patentu piešķiršanas un saistītās procedūrās (OV EPO 2021, A98) pielikuma 9. iedaļas a), d), h), i), j), l), m), n) un p) punktu.

([25]) Turklāt šajā gadījumā patenta pieteikums, iespējams, ir jānodod EPO no *PCT* līgumslēdzējas valsts centrālā rūpnieciskā īpašuma biroja vai citas kompetentās iestādes.

(12) Visbeidzot, EPO ir līgumi ar vairākiem pakalpojumu sniedzējiem Savienībā, kuri darbojas kā apstrādātāji Regulas (ES) 2016/679 4. panta 8. punkta nozīmē un nosūta personas datus EPO.

2.2. **Piemērojamais tiesiskais regulējums un datu aizsardzības noteikumi**

(13) Primārie tiesību akti, kas reglamentē EPO darbību, ir noteikti ar starptautisku līgumu, proti, ar Eiropas Patentu konvenciju vai ar Nolīgumu par sadarbību patentu jomā, ja EPO rīkojas saskaņā to. Otrajā EPO piemērojamo normu hierarhijas līmenī ir tiesību akti, ko pieņēmusi Administratīvā padome vai, kas attiecas uz *PCT*, *PCT* asambleja. EPO sekundārie tiesību akti ietver EPK īstenošanas noteikumus un tā dēvētos dienesta noteikumus (kas reglamentē ar EPO personālu saistītos aspektus, tostarp darbinieku tiesības un pienākumus) ([26]). Tiesības uz personas datu aizsardzību ir noteiktas dienesta noteikumu 1.B pantā ([27]), kas ietver arī dažus EPO datu aizsardzības regulējuma pamatnoteikumus, proti, attiecībā uz datu aizsardzības regulējuma piemērošanas jomu, īpašu kategoriju datu aizsardzību un personu tiesību īstenošanu. Dienesta noteikumu 2. panta 1. punktā un 32.A pantā ir paredzēti neatkarīgi pārraudzības mehānismi (datu aizsardzības speciālists (DAS) un Datu aizsardzības padome (DAP)), kam jāuzrauga atbilstība datu aizsardzības noteikumiem ([28]).

(14) Uz Administratīvo padomi un Iestādi, kā arī uz visām to struktūrvienībām attiecas vienas un tās pašas pamatprasības attiecībā uz personas datu aizsardzību. Konkrētāk, personas datu apstrādi Iestādē reglamentē Administratīvās padomes pieņemtie Eiropas Patentu iestādes pastāvīgo un citu darbinieku dienesta noteikumi par personas datu aizsardzību (datu aizsardzības noteikumi) 1.B un 32.A panta īstenošanas noteikumi ([29]). Uz personas datu apstrādi Administratīvajā padomē attiecas Administratīvās padomes datu aizsardzības noteikumi (AP DAN), kas piemēro DAN *mutatis mutandis* ([30]). Tur, kur šajā lēmumā ir atsauces uz DAN, tās ietver atbilstošās prasības, kas attiecas uz Administratīvo padomi, tās sekretariātu un komitejām. DAN struktūra un saturs ir cieši pieskaņots Savienības datu aizsardzības regulējumam ([31]). Konkrēti, tiem ir daudz kopīga ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 ([32]), kas nosaka datu aizsardzības prasības Savienības iestādēm un struktūrām un tādējādi ir labi piemērota starptautisko organizāciju specifiskajai struktūrai un iezīmēm, vienlaikus cieši atspoguļojot Regulu (ES) 2016/679.

([26]) EPK 33. pants.

([27]) Sk. jo īpaši dienesta noteikumu 1.B panta 1. punktu, kurā noteikts, ka "Iestāde cenšas nodrošināt, ka tiek ievērotas visu to personu pamattiesības uz privātumu un personas datu aizsardzību, kuru datus Iestāde apstrādā, un garantēt pārskatatbildību šajā ziņā." Sk. arī datu aizsardzības noteikumu (DAN) 1. panta 1. punktu, kurā paskaidrots, ka DAN ir paredzēts nepieciešamais tiesiskais regulējums, nodrošinātu, ka "tiek ievērotas fizisko personu pamattiesības uz privātumu un viņu personas datu, ko apstrādā Iestāde, aizsardzību".

([28]) Sk. arī DAN 47. un 48. punktu.

([29]) Datu aizsardzības noteikumi (no 495. lpp.), pieejami šeit: https://report-archive.epo.org/files/babylon/service_regulations_en.pdf. DAN attiecas arī uz Iestādes Apelācijas padomēm, izņemot pārsūdzības procedūru Datu aizsardzības padomē, kas neattiecas uz personas datu apstrādi, ko padomes veic, pildot tiesas funkcijas (DAN 2. panta 6. punkts). DAN ir noteikts, ka attiecībā uz šīm darbībām padomēm ir jāizveido atsevišķs neatkarīgs pārskatīšanas mehānisms.

([30]) Administratīvās padomes datu aizsardzības noteikumi, pieejami šeit: https://link.epo.org/ac-document/CA/D%202/23%20-%20En.pdf. Vienīgais aspekts, kurā Administratīvās padomes datu aizsardzības noteikumi atšķiras no DAN, ir pielāgojumi Administratīvās padomes konkrētajā struktūrā, t. i., atsauces uz Priekšsēdētāju tiek aizstātas ar atsaucēm uz Administratīvās padomes priekšsēdētāju. Turklāt tā dēvētajai Administratīvās padomes izraudzītajai komitejai ir pieņemti atsevišķi noteikumi – izraudzītās komitejas datu aizsardzības noteikumi (IK DAN). Šīs komitejas sastāvā ir EPO līgumslēdzējas valstis un lietotāju organizācijas, un tā ir izveidota ar Regulas (ES) Nr. 1257/2012 9. panta 2. punktu un EPK 145. pantu, lai uzraudzītu Iestādes darbību saistībā ar vienotā patenta procedūru. Ar izraudzītās komitejas datu aizsardzības noteikumiem personas datu apstrādei, ko veic izraudzītā komiteja, tiek piemēroti Administratīvās padomes datu aizsardzības noteikumi (ar kuriem savukārt tiek piemēroti DAN) (sk. https://link.epo.org/web/about-us/governance/SC_D_1_23_en.pdf). Arī šajā gadījumā izraudzītās komitejas datu aizsardzības noteikumi atšķiras no Administratīvās padomes un Iestādes noteikumiem tikai ar to, ka atsaucas uz komitejas priekšsēdētāju (nevis Padomes priekšsēdētāju vai Priekšsēdētāju).

([31]) EPO datu aizsardzības noteikumi: https://www.epo.org/en/about-us/office/data-protection-and-privacy.

([32]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(15) Priekšsēdētājs ir izdevis papildu juridiski saistošus instrumentus attiecībā uz datu apstrādi, ko veic Iestāde, piemēram, apkārtrakstus, lēmumus un iekšējos administratīvos norādījumus ([33]). Konkrēti, DAN ir papildināti ar Priekšsēdētāja 2021. gada 13. decembra lēmumu par personas datu apstrādi patentu piešķiršanas un ar to saistītās procedūrās (*PGP* lēmums) ([34]), 2022. gada 7. decembra lēmumu par personas datu apstrādi tiesvedībās, kas saistītas ar vienota spēka Eiropas patentiem (*UP* lēmums) ([35]), 2022. gada 17. novembra lēmumu par valstīm un vienībām, ko uzskata par tādām, kuras nodrošina personas datu pienācīgu aizsardzību ([36]), 2024. gada 2. maija lēmumu, ar ko nosaka Iestādes operatīvās vienības, kuras darbojas kā deleģētie pārziņi ([37]), kā arī Apkārtrakstu Nr. 420, ar ko īsteno DAN 25. pantu par datu subjektu tiesību ierobežojumiem (420. apkārtraksts) ([38]). Īpaši attiecībā uz datu apstrādi patentu piešķiršanas procedūru kontekstā ir svarīgi norādīt, ka personas datu apstrādes prasības, kas tieši paredzētas EPK un *PCT*, prevalē pār DAN. Mijiedarbība starp EPK un *PCT*, no vienas puses, un DAN, no otras puses, ir precizēta *PGP* lēmumā ([39]) un *UP* lēmumā. Konkrētās datu aizsardzības prasības, kas izriet tieši no EPK un *PCT*, ir izvērtētas 55.–59. apsvērumā. DAN un tos papildinošie instrumenti ir juridiski saistoši un izpildāmi, un privātpersonas uz tiem var atsaukties, izmantojot neatkarīgus tiesiskās aizsardzības mehānismus, kā aprakstīts 89.–96. apsvērumā.

(16) Noteikumi, kas paredzēti 15. apsvērumā minētajos juridiskajos instrumentos, ir iestrādāti datu aizsardzības inspektora izdotajos instrumentos (sk. 83.–88. apsvērumu) ([40]), kas attiecas uz Administratīvo padomi un Iestādi, kā arī uz visiem to departamentiem ([41]).

2.3. **Datu aizsardzības noteikumu materiālā darbības joma un darbības joma attiecībā uz personām**

(17) Saskaņā ar DAN un dienesta noteikumiem ([42]) visiem EPO darbiniekiem, apstrādājot personas datus, ir jāievēro DAN. DAN materiālo darbības jomu un darbības jomu attiecībā uz personām nosaka tajos definētie termini "personas dati", "apstrāde", "pārzinis", "deleģētais pārzinis" un "apstrādātājs".

2.3.1. ***Personas datu un apstrādes definīcija***

(18) "Personas datu" un "apstrādes" definīcijas DAN ir identiskas definīcijām Regulā (ES) 2016/679 ([43]). DAN attiecas uz jebkuru EPO veiktu personas datu apstrādi neatkarīgi no tā, vai šāda apstrāde attiecas uz tās darbinieku vai citu personu personas datiem ([44]). Dati, kas ir pseidonimizēti ([45]), arī tiek uzskatīti par personas datiem, savukārt mirušu

([33]) EPK 10. pants. Sk. arī DAN 1. panta 2. punkta a) apakšpunktu.

([34]) https://www.epo.org/en/legal/official-journal/2021/12/a98.html. Līdzīgu lēmumu ir pieņēmis Apelācijas padomju priekšsēdētājs attiecībā uz datu apstrādi apelācijas procesos Apelācijas padomēs, proti, 2023. gada 14. jūlija lēmums par personas datu apstrādi apelācijas procesos Apelācijas padomēs, pieejams šeit: https://www.epo.org/en/legal/official-journal/2023/07/a73.html.

([35]) 2022. gada 7. decembra Lēmums par personas datu apstrādi tiesvedībās, kas saistītas ar vienota spēka Eiropas patentiem, pieejams šeit: https://www.epo.org/en/legal/official-journal/2022/12/a112.html.

([36]) https://epo.org/en/legal/official-journal/2022/12/a111.html. Grozījumi izdarīti ar 2023. gada 11. maija lēmumu (OV Eiropas Patentu iestāde 2023, A57), pieejams šeit: https://www.epo.org/en/legal/official-journal/2023/06/a57.html.

([37]) https://link.epo.org/web/en-decision-of-the-president-on-delegated-controllers.pdf. Šo lēmumu atjaunina vismaz reizi gadā.

([38]) 420. apkārtraksts, ar ko īsteno datu aizsardzības noteikumu 25. pantu, pieejams šeit: https://link.epo.org/web/circular_420_en.pdf.

([39]) Attiecībā uz personas datu apstrādi, ko Apelācijas padomes veic apelācijas procesos, šī mijiedarbība ir precizēta Apelācijas padomju priekšsēdētāja lēmumā par personas datu apstrādi apelācijas procesos Apelācijas padomēs.

([40]) Sk., piemēram, atsauci uz DAI izdotajiem operatīvajiem dokumentiem DAN 1. panta 2. punkta c) apakšpunktā, kurus apstiprinājis Priekšsēdētājs un kuri tādējādi ir kļuvuši saistoši.

([41]) Sk. Administratīvās padomes DAN 1. panta 6. punktu un 12. panta 5. punktu.

([42]) DAN 2. panta 2. punkts un dienesta noteikumu 1. pants.

([43]) DAN 3. panta 1. punkta a) un b) apakšpunkts un VDAR 4. panta 1. un 2. punkts.

([44]) Dienesta noteikumu 1.B panta 2. punkts un DAN 2. panta 2. un 3. punkts. Sk. arī "datu subjekta" definīciju (DAN 3. panta 1. punkta w) apakšpunkts), proti, "jebkura identificēta vai identificējama fiziska persona neatkarīgi no tā, vai šī persona ir vai nav Iestādes darbinieks". Lai noteiktu, vai persona ir identificējama, ir jāņem vērā visi līdzekļi, ko pārzinis vai kāda cita persona pietiekami iespējami varētu izmantot – piemēram, atsevišķa izdalīšana –, lai tieši vai netieši identificētu fizisku personu.

([45]) Respektīvi, "personas datu apstrāde, ko veic tādā veidā, lai personas datus bez papildu informācijas izmantošanas vairs nebūtu iespējams attiecināt uz konkrētu datu subjektu, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek attiecināti uz identificētu vai identificējamu fizisku personu", sk. DAN 3. panta 1. punkta e) apakšpunktu.

vai juridisku personu dati vai anonīma informācija ([46]) saskaņā ar DAN netiek uzskatīta par personas datiem ([47]).

(19) DAN attiecas uz personas datu apstrādi, kas EPO pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un tādu personas datu apstrādi, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem ([48]).

2.3.2. ***Pārzinis, deleģētais pārzinis un apstrādātājs***

(20) DAN "pārzinis" ir definēts kā "vienība, proti, Eiropas Patentu iestāde, kas viena pati vai kopā ar citām nosaka personas datu apstrādes nolūkus un līdzekļus" ([49]). Principā kā Biroja veikto datu apstrādes darbību pārzinis darbojas Priekšsēdētājs ([50]). Tas pats attiecas uz Administratīvo padomi (kur kā pārzinis darbojas priekšsēdētājs), Apelācijas padomēm, kas pilda tiesas funkcijas (kur kā pārzinis darbojas to priekšsēdētājs ([51])), un uz izraudzīto komiteju (kur kā pārzinis darbojas priekšsēdētājs ([52])). Pārzinis var deleģēt šīs pilnvaras operatīvajām struktūrvienībām, ko pārstāv augstākā līmeņa vadītājs ([53]). Šādos gadījumos operatīvās vienības darbojas kā "deleģētie pārziņi" ([54]), kas definē apstrādes darbības nolūku (piemēram, iemeslu, pamatojumu un darbības vajadzības), tās līdzekļus un nodrošina, ka visas apstrādes darbības, kas saistītas ar personas datiem, atbilst DAN nosacījumiem ([55]). Šādos gadījumos pārzinis joprojām ir atbildīgs par personas datu apstrādi. DAN ir arī paredzēts "kopīgas pārzināšanas" scenārijs, kurā pārzinis nosaka apstrādes nolūku un līdzekļus kopā ar vienu vai vairākiem pārziņiem ārpus EPO ([56]).

([46]) Respektīvi, "informācija, kas neattiecas uz identificētu vai identificējamu fizisku personu vai personas datiem, ko sniedz anonīmi tādā veidā, ka datu subjekts nav vai vairs nav identificējams", sk. DAN 3. panta 1. punkta r) apakšpunktu. Saskaņā ar DAN 13. panta 1. punktu pārzinim nav jāglabā, jāiegūst vai jāapstrādā papildu informācija personas identificēšanai tikai nolūkā ievērot DAN, ja nolūkiem, kādos dati tiek apstrādāti, nav vai vairs nav nepieciešama personas identifikācija.

([47]) DAN 2. panta 4. punkts. Attiecībā uz personas datu apstrādi arhivēšanas nolūkos (likumīgi īstenojot EPO oficiālās pilnvaras), zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos DAN ir noteikts, ka ir jāievieš tehniski un organizatoriski pasākumi, lai tostarp nodrošinātu datu minimizēšanas principa ievērošanu un, ja šādi var sasniegt apstrādes nolūku, apstrādātu datus tādā veidā, ka identificēt personu vairs nav iespējams (DAN 14. pants).

([48]) Dienesta noteikumu 1.B panta 3. punkts un DAN 2. panta 1. punkts. "Kartotēka" ir definēta kā "jebkurš strukturēts personas datu kopums, kas ir pieejams saskaņā ar konkrētiem kritērijiem, neatkarīgi no tā, vai datu kopums ir centralizēts, decentralizēts vai izkliedēts, pamatojoties uz funkcionālu vai ģeogrāfisku motivāciju", sk. DAN 3. panta 1. punkta f) apakšpunktu.

([49]) DAN 3. panta 1. punkta g) apakšpunkts. Šajā lēmumā lietotais termins "pārzinis" attiecas vai nu uz pašu EPO, vai uz deleģētajiem pārziņiem.

([50]) EPK 10. panta 2. punkts un DAN 28. panta 1. punkts.

([51]) DAN 28. panta 2. punkts. Tas konkrēti izriet no Iestādes Priekšsēdētāja deleģētajām pilnvarām, sk. https://www.epo.org/en/legal/official-journal/2021/etc/se1/p175.html. Citu darbību gadījumā (ja padomes nerīkojas kā tiesu iestādes) padomju priekšsēdētājs darbojas kā deleģētais pārzinis Iestādes Priekšsēdētāja vārdā.

([52]) Sk. AP DAN 1. panta 4. punkta 5. apakšpunktu un izvēlētās komitejas reglamenta 13.a panta 2. punktu.

([53]) DAN 28. panta 3. punkts.

([54]) Sk. DAN 3. panta 1. punkta h) apakšpunktu. Personai, kas pārstāv operatīvo vienību, jābūt augstākā līmeņa vadītājam, parasti vismaz vienam no direktoriem. Deleģēto pārziņu saraksts ir publiskots (sk., piemēram, https://link.epo.org/web/decision_of_the_president_on_delegated_controllers_en.pdf un https://link.epo.org/web/decision_of_the_president_of_the_boards_of_appeal_appointing_a_delegated_controller_en.pdf) un tiek regulāri atjaunināts.

([55]) Ja šajā lēmumā minēts "pārzinis", tas ietver attiecīgos deleģētos pārziņus.

([56]) Šajā gadījumā DAN 29. pantā ir noteikts, ka (deleģētajam) pārzinim pārredzamā veidā ir jānosaka abu pušu attiecīgie pienākumi attiecībā uz savu datu aizsardzības pienākumu izpildi, sevišķi attiecībā uz fizisku personu tiesību īstenošanu un pārredzamības pienākumiem.

(21) "Apstrādātāja" definīcija DAN ir identiska definīcijai Regulas (ES) 2016/679 4. panta 8. punktā, t. i., fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus ([57]). Pārzinim ir atļauts izmantot tikai apstrādātājus, kuri sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu, ka apstrāde atbilst DAN prasībām ([58]). Attiecības starp pārzini un apstrādātāju jāreglamentē ar līgumu vai juridisku aktu, kas ir apstrādātājam saistošs un tostarp nosaka apstrādes priekšmetu, ilgumu, būtību un nolūku ([59]). Apstrādātājam ir atļauts apstrādāt datus tikai pēc dokumentētiem pārziņa norādījumiem. Apstrādātājam ir jāpalīdz pārzinim pildīt savus pienākumus saskaņā ar DAN. Apstrādātājam ir aizliegts iesaistīt apakšapstrādātājus bez pārziņa iepriekšējas atļaujas ([60]). Deleģētajiem pārziņiem ir pieejams standarta datu apstrādes līgums ([61]). Turklāt, ja apstrādātājs atrodas trešā valstī, jebkurai personas datu kopīgošanai ar šo apstrādātāju ir jāatbilst arī DAN prasībām attiecībā uz starptautisku nosūtīšanu, kā aprakstīts šā lēmuma 68.–73. apsvērumā ([62]).

2.4. **Aizsardzības pasākumi, tiesības un pienākumi**

2.4.1. ***Apstrādes likumīgums un godprātība***

(22) Personas dati būtu jāapstrādā likumīgi un godprātīgi.

(23) Minētie vispārīgie principi ir noteikti DAN 4. panta 2. punkta a) apakšpunktā tā, ka to var uzskatīt par identisku Regulas (ES) 2016/679 5. panta 1. punkta a) apakšpunktam.

(24) Likumības princips ir sīkāk izklāstīts DAN 5. pantā, kurā uzskaitīti juridiskie pamati, uz kuru bāzes var apstrādāt personas datus. Minētie juridiskie pamati ir a) nepieciešamība veikt uzdevumu, īstenojot EPO oficiālās darbības ([63]) vai likumīgi īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras, kas ietver apstrādi, kura nepieciešama Iestādes pārvaldībai un darbībai ([64]); b) nepieciešamība izpildīt juridisku pienākumu, kas attiecas uz pārzini (piemēram, publicēt patenta pieteikumā minēto informāciju Eiropas Patentu reģistrā ([65])); c) nepieciešamība pildīt līgumu, kura līgumslēdzēja puse ir datu subjekts, vai pēc datu subjekta pieprasījuma veikt pasākumus pirms līguma noslēgšanas; d) datu subjekta piekrišana; e) nepieciešamība aizsargāt datu subjekta vai citas fiziskas personas vitālas intereses.

([57]) DAN 3. panta 1. punkta j) apakšpunkts.
([58]) DAN 30. panta 1. punkts.
([59]) DAN 30. panta 3. punkts.
([60]) DAN 30. panta 2. un 3. punkts. Apstrādātājam, kas iesaista apakšapstrādātāju, (līgumiski) ir jānosaka apakšapstrādātājam tādi paši datu aizsardzības pienākumi kā tie, kas paredzēti līgumā starp pārzini un apstrādātāju (DAN 30. panta 4. punkts).
([61]) EPO vispārējo līguma noteikumu E pielikums, https://link.epo.org/web/general_conditions_of_contract_en.pdf.
([62]) 8. panta 1., 2. un 5. punkts kopā ar DAN 9. panta 1. punktu.
([63]) Tas attiecas uz uzdevumiem, ko veic saskaņā ar EPK un *PCT* vai uz to pamata pieņemtiem noteikumiem (piemēram, dienesta noteikumiem), kuri ir nepieciešami EPO uzdevumu veikšanai patentu piešķiršanas procedūrā. Sk. arī *PGP* lēmuma pielikuma 5. punkta 1. apakšpunktu un attiecīgos EPK noteikumus, piemēram, to IV un V daļu. Lai veiktu EPI uzdevumus saistībā ar patentu piešķiršanas procedūru, EPI apstrādā personas datus, lai: apstrādātu pieteikumus un patentus; veiktu iebildumu izskatīšanas procedūras; sazinātos ar procesā iesaistītajām pusēm (un attiecīgā gadījumā ar trešām personām); uzturētu Eiropas Patentu reģistru; sagatavotu ziņojumus un statistiku un apmainītos ar datiem ar līgumslēdzējām valstīm un Pasaules Intelektuālā īpašuma organizāciju (*PGP* lēmuma pielikuma 6. punkts).
([64]) Tas aptver Iestādes Priekšsēdētājam uzticētos uzdevumus: nodrošināt Iestādes efektīvu darbību un pārvaldību. Sk., piemēram, EPK 10. pantu, kurā aprakstīti Priekšsēdētāja uzdevumi attiecībā uz personālu, (piekļuvi) ēkām un aprīkojuma pārvaldību. Šāda pieeja atbilst Regulas (ES) 2018/1725 5. panta 1. punkta a) apakšpunktam un 22. apsvērumam. Tas attiecas arī uz Administratīvās padomes uzdevumiem saskaņā ar EPK, piemēram, izstrādāt noteikumus par pensijām un finanšu noteikumiem, sk. EPK 33. pantu, EPK īstenošanas noteikumu 9. panta 2. punktu, 12. panta c) punktu un 122. panta 4. punktu. Attiecībā uz izraudzīto komiteju tas attiecas uz uzraudzības uzdevumiem saskaņā ar EPK 145. pantu. Visbeidzot, attiecībā uz Apelācijas padomēm tas attiecas, piemēram, uz tās atbildību izskatīt apelācijas par citu Iestādes daļu lēmumiem, sk. EPK 21. panta 1. punktu.
([65]) Sk., piemēram, EPK īstenošanas noteikumu 20. pantu.

(25) Piekrišana DAN ir definēta tāpat kā Regulā (ES) 2016/679, proti, "jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei" ([66]). Pārzinim ir jāpierāda, ka datu subjekts ir piekritis ([67]). Novērtējot to, vai piekrišana ir dota brīvi, būtu jāņem vērā tas, vai līguma izpilde ir atkarīga no piekrišanas tādai datu apstrādei, kura nav nepieciešama minētā līguma izpildei ([68]). Piekrišana nevar tikt uzskatāma par brīvi izteiktu, ja datu subjektam nav īstas vai brīvas izvēles, vai viņš nevar atteikties vai atsaukt savu izvēli bez nelabvēlīgām sekām ([69]). Turklāt DAN nosaka, ka, lai piekrišana būtu apzināta, datu subjektam jābūt informētam vismaz par pārziņa identitāti un paredzētās personas datu apstrādes nolūkiem ([70]). Visbeidzot, datu subjektam ir tiesības jebkurā laikā piekrišanu atsaukt ([71]).

2.4.2. *Īpašu kategoriju datu apstrāde*

(26) Būtu vajadzīgi īpaši aizsardzības pasākumi gadījumos, kad tiek apstrādāti "īpašu kategoriju" dati.

(27) DAN ir ietverti sevišķi noteikumi par tādu īpašu kategoriju personas datu apstrādi ([72]), kas ir definēti tāpat kā Regulā (ES) 2016/679, proti, personas dati, "kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētiskie dati ([73]), biometriskie dati ([74]), lai veiktu fiziskas personas unikālu identifikāciju, veselības dati ([75]) vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju" ([76]). Saskaņā ar DAN īpašu kategoriju datu apstrāde principā ir aizliegta, ja vien nav piemērojams īpašs izņēmums ([77]).

(28) DAN 11. panta 2. punktā uzskaitītie īpašie izņēmumi ir līdzīgi Regulas (ES) 2016/679 9. panta 2. un 3. punktā minētajiem izņēmumiem ar dažiem pielāgojumiem tiesiskajā regulējumā, kurā darbojas EPO. Īpašu kategoriju personas datu apstrāde ir atļauta tikai konkrētos un ierobežotos apstākļos ([78]), t. i., ja 1) datu subjekts ir devis nepārprotamu piekrišanu, 2) apstrāde ir vajadzīga, lai aizsargātu personas vitālas intereses (ja datu subjekts ir fiziski vai tiesiski nespējīgs dot nepārprotamu piekrišanu), 3) datu subjekts ir acīmredzami publiskojis šos personas datus,

([66]) DAN 3. panta 1. punkta m) apakšpunkts. Sk. arī DAN 7. panta 2. punktu.
([67]) DAN 7. panta 1. punkts.
([68]) DAN 7. panta 1., 5., 6. un 7. punkts.
([69]) DAN 7. panta 4. punkts.
([70]) DAN 7. panta 4. punkts.
([71]) DAN 7. panta 5. punkts.
([72]) Sk., piemēram, DAN 11. pantu.
([73]) Definēti kā "personas dati, kas attiecas uz fiziskas personas pārmantotajām vai iegūtajām ģenētiskajām pazīmēm, sniedz unikālu informāciju par minētās fiziskās personas fizioloģiju vai veselību un kas izriet jo īpaši no attiecīgās fiziskās personas bioloģiskā parauga analīzes", sk. DAN 3. panta 1. punkta o) apakšpunktu.
([74]) Definēti kā "personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopiskie dati," sk. DAN 3. panta 1. punkta p) apakšpunktu.
([75]) Respektīvi, personas dati, kas saistīti ar fiziskas personas fizisko vai garīgo veselību, tostarp veselības aprūpes pakalpojumu sniegšanu, un kas atspoguļo informāciju par tās veselības stāvokli, sk. DAN 3. panta 1. punkta q) apakšpunktu.
([76]) DAN 11. panta 1. punkts.
([77]) DAN 11. panta 1. un 2. punkts.
([78]) DAN arī ļauj apstrādāt īpašu kategoriju datus konkrētās situācijās, kas galvenokārt ir saistītas ar EPO darbiniekiem un tāpēc mazāk attiecas uz datiem, kuri nosūtīti, pamatojoties uz šo lēmumu. Konkrēti, īpašu kategoriju datus var apstrādāt, ja to atļauj juridiski saistošs noteikums, kas attiecas uz Eiropas Patentu organizāciju (piemēram, EPK un Administratīvās padomes un Priekšsēdētāja pieņemtie instrumenti, sk. DAN 3. panta 1. punkta y) apakšpunktu), kas paredz atbilstošus aizsardzības pasākumus datu subjekta pamattiesībām un interesēm (DAN 11. panta 2. punkta b) apakšpunkts) un ir nepieciešams, lai izpildītu pārziņa vai datu subjekta pienākumus un īstenotu īpašas tiesības nodarbinātības un sociālā nodrošinājuma tiesību jomā. Apstrāde var notikt arī tad, ja tā ir vajadzīga sabiedrības interešu dēļ sabiedrības veselības jomā (piemēram, aizsardzībai pret nopietniem pārrobežu draudiem veselībai vai augstu kvalitātes un drošības standartu nodrošināšanai, pamatojoties uz valsts tiesību aktiem, kas paredz atbilstošus un konkrētus pasākumus datu subjekta tiesību un brīvību, jo īpaši dienesta noslēpuma, aizsardzībai, sk. DAN 11. panta 2. punkta g) apakšpunktu). Visbeidzot, apstrāde var būt nepieciešama profilaktiskai medicīnai vai arodmedicīnai, darbinieka darbspējas novērtēšanai, medicīniskai diagnozei, veselības vai sociālās aprūpes sniegšanai vai ārstēšanai, veselības vai sociālās aprūpes sistēmu un pakalpojumu pārvaldībai vai medicīniskajām pārbaudēm un atzinumiem, ja šos datus apstrādā veselības nozares darbinieks, uz kuru attiecas pienākums glabāt dienesta noslēpumu, vai cita persona, uz kuru attiecas līdzvērtīgs pienākums ievērot slepenību (DAN 11. panta 3. punkts).

4) apstrāde ir vajadzīga konkrētam nolūkam, kas saistīts ar EPO oficiālo darbību veikšanu, vai pārzinim likumīgi piešķirto pilnvaru īstenošanai ([79]) vai 5) apstrāde ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības.

(29) Papildus īpašajām personas datu kategorijām, kas minētas 27. apsvērumā, DAN ir paredzēta arī īpaša aizsardzība tādu personas datu apstrādei, kas attiecas uz sodāmību un noziedzīgiem nodarījumiem, proti, šāda apstrāde ir atļauta tikai pēc iepriekšējas apspriešanās ar DAP vai ja apstrāde ir prasīta juridiski saistošā instrumentā, kas paredz atbilstošus aizsardzības pasākumus personu tiesībām un brīvībām ([80]).

2.4.3. ***Nolūka ierobežojums***

(30) Personas dati būtu jāapstrādā konkrētā nolūkā, un pēc tam tos var izmantot, ciktāl tas nav pretrunā apstrādes nolūkam.

(31) Šis princips ir nostiprināts DAN 4. panta 2. punkta b) apakšpunktā, saskaņā ar kuru personas datus "vāc konkrētos, skaidros un leģitīmos nolūkos un tos turpmāk neapstrādā veidā, kas nav savienojams ar šiem nolūkiem".

(32) Līdzīgi kā Regulā (ES) 2016/679 DAN atļauj turpmāku apstrādi (neatkarīgi no turpmākās apstrādes nolūka saderības ar sākotnējo), pamatojoties uz datu subjekta nepārprotamu piekrišanu vai pamatojoties uz piemērojamām EPO tiesību normām ([81]). Par pēdējo minēto gadījumu DAN ir noteikts, ka apstrādei jābūt nepieciešamam un samērīgam pasākumam vispārēju sabiedrības interešu aizsardzības nolūkā ([82]).

(33) Ja turpmāka apstrāde nav balstīta uz šiem diviem pamatiem, DAN ir paredzēti faktori, kas jāņem vērā, novērtējot turpmākas apstrādes nolūka saderību ar nolūku, kādam personas dati sākotnēji tika vākti ([83]). Šī pieeja un DAN uzskaitītie faktori ir identiski tiem, kas noteikti Regulas (ES) 2016/679 6. panta 4. punktā un Regulas (ES) 2018/1725 ([84]) 6. pantā.

2.4.4. ***Datu precizitāte un minimizēšana, glabāšanas ierobežojumi un datu drošība***

(34) Personas datiem vajadzētu būt precīziem un vajadzības gadījumā atjauninātiem. Tiem vajadzētu būt arī adekvātiem, atbilstīgiem un nevajadzētu būt pārmērīgiem, ņemot vērā nolūkus, kādos tie tiek apstrādāti, un tie principā nebūtu jāglabā ilgāk nekā nepieciešams nolūkiem, kādos personas datus apstrādā.

(35) Šie principi ir noteikti DAN 4. panta 2. punkta c), d) un e) apakšpunktā tāpat kā Regulā (ES) 2016/679.

([79]) Piemēram, saistībā ar apelācijām pret piešķirtu patentu konfidenciāli dati varētu būt iekļauti liecinieku liecībās vai iesniegtajos pierādījumos. Apstrāde saskaņā ar šo noteikumu var notikt arī tad, ja tas ir būtiski nepieciešams Iestādes pārvaldībai un darbībai un pienākumiem, kas izriet no EPO pienākuma sadarboties ar līgumslēdzējām valstīm (piemēram, vajadzība apstrādāt personāla vai apmeklētāju veselības informāciju saskaņā ar prasībām, ko noteikušas EPO uzņēmējas valsts sabiedrības veselības iestādes). Jebkurā gadījumā juridiskajam instrumentam, kas ir apstrādes pamatā, ir jābūt samērīgam ar sasniedzamo mērķi, jāievēro tiesību uz datu aizsardzību būtība un jāparedz piemēroti un konkrēti pasākumi datu subjekta pamattiesību un interešu aizsardzībai (DAN 11. panta 2. punkta f) apakšpunkts).

([80]) DAN 12. pants. Iespējamais scenārijs, kurā šādi dati tiktu apstrādāti, ietver disciplinārlietas attiecībā uz patentu advokātiem EPO Disciplinārlietu kolēģijā (sk., piemēram, *PGP* lēmuma pielikuma A.7. punktu).

([81]) DAN 6. panta 2. punkts.

([82]) Piemēram, organizācijas drošība; noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana vai kriminālvajāšana; citu tiesības un brīvības utt. (Sk. DAN 25. panta 1. punktu).

([83]) DAN 6. panta 3. punkts.

([84]) Konkrēti – jebkura saikne starp nolūkiem, kādos personas dati ir vākti, un paredzētās turpmākās apstrādes nolūkiem; konteksts, kādā dati tika vākti; datu raksturs; turpmākās apstrādes iespējamās sekas fiziskām personām, sk. DAN 6. panta 3. punktu.

(36) Personas dati arī būtu jāapstrādā tā, ka tiek nodrošināta to drošība, kas ietver aizsardzību pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu. Tālab uzņēmējiem būtu jāveic atbilstoši tehniskie vai organizatoriskie pasākumi, lai aizsargātu personas datus no iespējamiem apdraudējumiem. Šie pasākumi būtu jānovērtē, ņemot vērā faktisko situāciju un saistītās izmaksas.

(37) Datu drošība ir nostiprināta EPO tiesiskajā regulējumā, izmantojot integritātes un konfidencialitātes principu, kas noteikts DAN 4. panta 2. punkta f) apakšpunktā un 33. pantā, gandrīz tādā pašā veidā kā Regulā (ES) 2016/679. Konkrēti, DAN ir noteikts, ka ar atbilstošiem tehniskiem un organizatoriskiem pasākumiem tiek nodrošināts riskam atbilstošs drošības līmenis, ņemot vērā jaunākos sasniegumus, īstenošanas izmaksas un apstrādes raksturu, tvērumu, kontekstu un nolūkus, kā arī risku atšķirīgo iespējamību un nopietnību attiecībā uz personu tiesībām un brīvībām.

(38) Turklāt DAN ir ietvertas īpašas prasības attiecībā uz rīcību datu aizsardzības pārkāpuma gadījumā un paziņošanu par to ([85]). Pirmkārt, pārzinim bez nepamatotas kavēšanās (un, ja iespējams, ne vēlāk kā 72 stundu laikā pēc tam, kad tas uzzinājis par datu aizsardzības pārkāpumu) ir jāpaziņo DAS par datu aizsardzības pārkāpumu, izņemot, ja iespēja, ka pārkāpums varētu radīt risku personu tiesībām un brīvībām, ir maz ticama ([86]). Tāpat apstrādātājam bez liekas kavēšanās ir jāpaziņo pārzinim par pārkāpumu ([87]). Paziņojumā jāapraksta pārkāpuma raksturs, tā iespējamās sekas un pasākumi, kas veikti vai ko ierosināts veikt, lai pārkāpumu novērstu ([88]). Ja datu aizsardzības pārkāpums varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinim bez kavēšanās jāpaziņo datu subjektam par personas datu aizsardzības pārkāpumu ([89]). Paziņojumā datu subjektam skaidrā un vienkāršā valodā jāapraksta personas datu aizsardzības pārkāpuma raksturs ([90]), taču tas nav nepieciešams, ja pārzinis ir veicis turpmākus pasākumus, kas nodrošina, ka augstais risks datu subjektu tiesībām un brīvībām vairs nepastāv ([91]).

2.4.5. ***Pārredzamība***

(39) Datu subjektiem vajadzētu būt informētiem par viņu personas datu apstrādes galvenajām iezīmēm.

(40) Saskaņā ar DAN pārzinim personas datu iegūšanas brīdī ir jāsniedz fiziskām personām šāda informācija: sava identitāte un kontaktinformācija (kā arī DAS kontaktinformācija), apstrādes nolūks un juridiskais pamats, saņēmēji vai saņēmēju kategorijas, tas, ka tiek plānots nosūtīt datus ārpus EPO, kā arī piemērojamās tiesības un iespēja lēmumu pārsūdzēt ([92]). Tas pats attiecas uz gadījumiem, kad personas datus apstrādā citā nolūkā, nevis tajā, kādā dati tika vākti ([93]). Abi pienākumi ir piemērojami tikai tad, ja attiecīgajai personai vēl nav minētās informācijas ([94]).

(41) Tāda pati informācija ir jāsniedz datu subjektiem, ja personas dati netiek vākti tieši no viņiem, kopā ar papildu informāciju par personas datu avotu un attiecīgajām datu kategorijām ([95]). Šī informācija ir jāsniedz saprātīgā termiņā pēc datu iegūšanas (bet vēlākais mēneša laikā), ņemot vērā konkrētos apstākļus, kādos dati tiek apstrādāti ([96]). Ja personas dati ir jāizmanto saziņai ar datu subjektu, tā pati informācija būtu jāsniedz vēlākais brīdī, kad notiek pirmā saziņa ar attiecīgo personu ([97]). 40. apsvērumā minētā informācija ir jāsniedz arī pirms jebkādas turpmākas apstrādes vai, ja ir paredzēta izpaušana citam saņēmējam, ne vēlāk kā tad, kad personas dati tiek izpausti trešai personai ([98]). Minētais pienākums neattiecas uz vairākiem gadījumiem, proti, ja datu subjekta rīcībā jau ir

([85]) "Datu aizsardzības pārkāpums" ir definēts kā "drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem", sk. DAN 3. panta 1. punkta n) apakšpunktu.
([86]) DAN 34. panta 1. punkts.
([87]) DAN 34. panta 2. punkts.
([88]) DAN 34. panta 1. un 3. punkts.
([89]) DAN 34. panta 6. punkts.
([90]) DAN 34. panta 6. punkts.
([91]) DAN 34. panta 8. punkts.
([92]) DAN 16. panta 1. un 2. punkts.
([93]) DAN 16. panta 3. punkts.
([94]) DAN 16. panta 4. punkts.
([95]) DAN 17. panta 1. un 2. punkts.
([96]) DAN 17. panta 3. punkta a) apakšpunkts.
([97]) DAN 17. panta 3. punkta b) apakšpunkts.
([98]) DAN 17. panta 3. punkta c) apakšpunkts un 4. punkts. Trešā persona DAN 3. panta 1. punkta l) apakšpunktā ir definēta kā "jebkura fiziska vai juridiska persona, valsts iestāde, aģentūra vai struktūra, kura nav ne datu subjekts, ne pārzinis, ne apstrādātājs un arī ne persona, kura ir pilnvarota apstrādāt personas datus pārziņa vai apstrādātāja tiešā vadībā".

attiecīgā informācija, ja šai informācijai jāpaliek konfidenciālai dienesta noslēpuma glabāšanas pienākuma dēļ, ko reglamentē EPK un/vai citas EPO piemērojamās tiesību normas ([99]), ja minētās informācijas sniegšana izrādās neiespējama vai būtu saistīta ar nesamērīgām pūlēm, sevišķi attiecībā uz apstrādi arhivēšanas, zinātnisku vai vēsturisku pētījumu vai statistikas vajadzībām, ciktāl tā padarītu neiespējamu vai nopietni kavētu apstrādes mērķu sasniegšanu, vai ja minētās informācijas iegūšana vai izpaušana ir skaidri noteikta EPK vai citās piemērojamās tiesību normās, kas paredz atbilstošus pasākumus datu subjekta likumīgo interešu aizsardzībai ([100]).

2.4.6. ***Individuālās tiesības***

(42) Datu subjektiem vajadzētu būt noteiktām tiesībām, kas ir īstenojamas attiecībā uz pārzini vai apstrādātāju, jo īpaši tiesībām piekļūt datiem, tiesībām uz datu labošanu, tiesībām iebilst pret apstrādi un tiesībām uz datu dzēšanu. Tajā pašā laikā uz šādām tiesībām var attiecināt ierobežojumus, ciktāl šie ierobežojumi ir nepieciešami un samērīgi, lai aizsargātu svarīgus vispārējo sabiedrības interešu mērķus.

2.4.6.1. *DAN nodrošinātās tiesības*

(43) Nepieciešamība atvieglot individuālo tiesību īstenošanu ir noteikta dienesta noteikumu 1.B panta 4. punktā. Lai tālāk īstenotu šo prasību, DAN piešķir personām tādas pašas tiesības kā Regulā (ES) 2016/679 noteiktās, proti, piekļuves tiesības (DAN 18. pants), tiesības uz labošanu (DAN 19. pants), tiesības uz dzēšanu (DAN 20. pants), tiesības uz apstrādes ierobežošanu (DAN 21. pants), tiesības uz datu pārnesamību (DAN 22. pants), tiesības iebilst (DAN 23. pants) un tiesības netikt pakļautam automatizētai lēmumu pieņemšanai (DAN 24. pants).

(44) DAN ir paredzēti arī vispārīgi noteikumi par fizisku personu tiesību īstenošanas pieprasījumu izskatīšanu, kur pārzinim tiek pieprasīts sazināties ar datu subjektiem, izmantojot skaidru un vienkāršu valodu, kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā (rakstiski vai ar citiem līdzekļiem) ([101]). Pārzinim bez liekas kavēšanās un jebkurā gadījumā viena mēneša laikā pēc pieprasījuma saņemšanas ir jāsniedz fiziskām personām informācija par pasākumiem, kas veikti, reaģējot uz pieprasījumu (ko vajadzības gadījumā var pagarināt vēl par diviem mēnešiem, ņemot vērā pieprasījumu sarežģītību un daudzumu) ([102]). Ja datu subjekta pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, jo īpaši to regulāras atkārtošanās dēļ, pārzinis var atteikties izpildīt pieprasījumu ([103]). Ja pārzinis neizpilda pieprasījumu, viņam par to jāinformē attiecīgā persona un jāsniedz informācija par iespēju lēmumu pārsūdzēt ([104]).

([99]) DAN 17. panta 4. punkts. Šādas konfidencialitātes prasības piemēro, piemēram, saistībā ar darbinieku personas datu apstrādi EPO medicīnas dienestā (tādā gadījumā uz konkrētajiem ārstiem var attiekties pienākums glabāt dienesta noslēpumu, sk., piemēram, DAN 11. panta 3. punktu un dienesta noteikumu 83.a, 84. un 84.a panta īstenošanas noteikumu E punktu) vai darbā pieņemšanas procedūru kontekstā (II pielikuma "Konkursa procedūras amatiem, kuros iecēlējinstitūcija ir Priekšsēdētājs" 6. iedaļa).

([100]) Proti, ja EPK vai uz tās pamata pieņemtie juridiskie instrumenti īpaši reglamentē privātpersonām vai sabiedrībai izpaužamo informāciju, sīkāk sk. 1.4.6.7. iedaļā.

([101]) DAN 15. panta 1. punkts.

([102]) DAN 15. panta 2. punkts.

([103]) DAN 15. panta 4. punkts. Turklāt DAN 13. panta 2. punktā ir precizēts, ka, ja pārzinis var pierādīt, ka nespēj identificēt datu subjektu, noteikumi par individuālajām tiesībām nav piemērojami (ja vien datu subjekts nesniedz papildu informāciju, kas ļauj viņu identificēt).

([104]) DAN 15. panta 3. punkts.

(45) Pirmkārt, attiecībā uz piekļuves tiesībām DAN nodrošina personām tiesības saņemt no EPO apstiprinājumu par to, vai viņu personas dati tiek vai netiek apstrādāti, un, ja tiek, piekļūt personas datiem vienkārši ([105]) un samērīgos intervālos ([106]). Turklāt personām ir tiesības iegūt šādu informāciju: apstrādes nolūks, attiecīgo datu kategorijas, saņēmēji, ar kuriem dati tiek kopīgoti, un paredzētais laikposms, kurā dati tiks glabāti ([107]).

(46) Otrkārt, DAN ir paredzēts, ka DAN paredzētās tiesības uz labošanu ļauj personām panākt neprecīzu datu labošanu vai nepilnīgu datu papildināšanu (piemēram, sniedzot papildu paziņojumu) ([108]). Kad datu labošana ir veikta, pārzinim tas jāpaziņo katram saņēmējam, kuram personas dati ir izpausti ([109]). Saskaņā ar DAN tiesības uz labošanu attiecas uz objektīviem un faktiskiem datiem, nevis uz subjektīviem apgalvojumiem ([110]), lai gan šajā gadījumā personām ir atļauts papildināt esošos datus ar citu viedokli vai cita eksperta atzinumu, vai sniegt komentārus ([111]).

(47) Treškārt, DAN arī piešķir personām tiesības uz dzēšanu ([112]), jo īpaši, ja a) personas dati vairs nav nepieciešami nolūkam, kādā tie tiek apstrādāti, b) datu subjekts atsauc piekrišanu un apstrādei nav cita juridiskā pamata, c) datu subjekts iebilst pret apstrādi, un apstrādei nav sevišķi svarīgu leģitīmu iemeslu, d) dati ir apstrādāti nelikumīgi vai e) dati ir jādzēš, lai izpildītu juridisku pienākumu, kas attiecas uz pārzini ([113]). Pārzinim ir jāpaziņo par dzēšanu katram saņēmējam, ar kuru dati ir kopīgoti, ja vien tas nav neiespējami vai nav saistīts ar nesamērīgām pūlēm ([114]). Tāpat, ja pārzinis ir publiskojis personas datus, tam ir jāveic saprātīgi pasākumi, lai informētu citus pārziņus, kas tos apstrādā, ka persona ir pieprasījusi dzēšanu ([115]). Tiesības uz dzēšanu neattiecas uz šādiem scenārijiem, ciktāl datu apstrāde ir nepieciešama, lai a) īstenotu tiesības uz vārda un informācijas brīvību, b) izpildītu EPO juridisku pienākumu vai pienākumu, kas izriet no EPO pienākuma sadarboties ar līgumslēdzējām valstīm ([116]), vai lai īstenotu EPO likumīgi piešķirtās oficiālās pilnvaras ([117]), c) lai sadarbotos ar līgumslēdzējām valstīm sabiedrības veselības jomā ([118]), d) arhivēšanas, zinātniskās vai vēstures pētniecības un statistikas nolūkos (ciktāl dzēšana varētu padarīt neiespējamu vai nopietni traucēt apstrādes mērķu sasniegšanu) vai e) lai celtu, īstenotu vai aizstāvētu juridiskas prasības ([119]).

([105]) Konkrētāk, pārzinim ir jānodrošina apstrādē esošo datu un visas pieejamās informācijas (jebkāda veida, neatkarīgi no tās rakstura (objektīvs vai subjektīvs), satura (tostarp jebkādas veiktās darbības) vai formāta (dokumenti uz papīra, datorā, e-pasti)) kopija saprotamā formā, sk. DAN 18. panta 3. punktu. Tajā pašā laikā tiesības saņemt datu kopiju nedrīkst negatīvi ietekmēt citu personu tiesības un brīvības (DAN 18. panta 5. punkts).

([106]) DAN 18. panta 1. punkts.

([107]) DAN 18. panta 2. un 3. punkts.

([108]) DAN 19. panta 1. punkts.

([109]) DAN 19. panta 3. punkts. Ja datu subjekts to pieprasa, pārzinim ir jāinformē, kas ir šie saņēmēji.

([110]) Šī interpretācija tika pieņemta saskaņā ar EDAU Pamatnostādnēm par personu tiesībām attiecībā uz personas datu apstrādi: https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf. Sk. jo īpaši norādījumus 18. lpp. par tiesībām labot datus un par "objektīviem un faktiskiem datiem" un "subjektīviem apgalvojumiem".

([111]) DAN 19. panta 2. punkts.

([112]) Datu dzēšana ir definēta kā "glabāto datu iznīcināšana tādā veidā, ka atjaunošana nav iespējama" (DAN 3. panta 1. punkta v) apakšpunkts). Atsauce uz "glabātiem datiem" attiecas uz visiem pārziņa (un jebkuru trešo personu pārziņa vārdā) savāktajiem un turētajiem datiem.

([113]) DAN 20. panta 1. punkts.

([114]) DAN 20. panta 4. punkts.

([115]) DAN 20. panta 2. punkts.

([116]) Saskaņā ar 20. pantu EPO Protokolā par privilēģijām un imunitāti var prasīt, lai EPO sniegtu personas datus savām līgumslēdzējām valstīm saistībā ar administratīviem vai tiesas procesiem, piemēram, attiecībā uz darbinieku pensijas tiesību aprēķināšanu un nodošanu, nodokļu izmeklēšanu vai saistībā ar civilprocesiem, kas attiecas uz EPO personālu.

([117]) Tas attiecas uz situācijām, kad EPO saskaņā ar EPK, *PCT* vai uz to pamata pieņemtiem juridiskiem instrumentiem ir jāapstrādā personas dati saistībā ar patentu piešķiršanas procedūru (piemēram, uzturot informāciju Eiropas Patentu reģistrā un Eiropas Patentu biļetenā saskaņā ar EPK 127. un 129. pantu).

([118]) Veselības datu apstrādei sabiedrības interešu dēļ sabiedrības veselības jomā ir jānotiek saskaņā ar DAN 11. panta 2. punkta g) apakšpunktu.

([119]) DAN 20. panta 3. punkts.

(48) Ceturtkārt, DAN 21. pantā ir paredzētas tiesības uz apstrādes ierobežošanu, proti, personas datu iezīmēšanu ar mērķi ierobežot to apstrādi nākotnē (tostarp programmēšanas pasākumiem, lai pastāvīgi liegtu piekļuvi šādiem datiem) ([120]). Konkrēti, uz šīm tiesībām var atsaukties, ja persona apstrīd personas datu precizitāti (uz laiku, kas pārzinim vajadzīgs, lai precizitāti pārbaudītu) vai ja apstrāde ir nelikumīga, bet persona iebilst pret datu dzēšanu ([121]). Ja apstrāde ir ierobežota, personas datus, izņemot glabāšanu, var apstrādāt tikai ar personas nepārprotamu piekrišanu, lai celtu, īstenotu vai aizstāvētu juridiskas prasības, aizsargātu citu personu tiesības vai izpildītu uzdevumu, ko veic, īstenojot EPO oficiālās darbības (t. i., uzdevumu, kas ir nepieciešams administratīvajam un tehniskajam darbam, kas EPO jāveic saskaņā ar EPK) ([122]).

(49) Piektkārt, tiesības iebilst ir noteiktas dienesta noteikumu 1.B panta 4. punktā un DAN 23. pantā. Konkrēti, fiziskām personām ir tiesības jebkurā laikā iebilst pret personas datu apstrādi, ko veic, lai izpildītu uzdevumu, īstenojot EPO oficiālās darbības vai likumīgi īstenojot pārzinim piešķirtās oficiālās pilnvaras ([123]). Personas ir jāinformē par šādu tiesību esamību skaidri un ne vēlāk kā pie pirmās saziņas ar tām ([124]). Ja persona iebilst pret personas datu apstrādi, DAN ir noteikts, ka pārzinim ir jāpārtrauc apstrāde, izņemot gadījumus, kad pārzinis spēj pierādīt pārliecinošus leģitīmus apstrādes iemeslus, kas ir svarīgāki par datu subjekta interesēm, tiesībām un brīvībām, vai arī kad jāceļ, jāīsteno vai jāaizstāv juridiskas prasības ([125]).

(50) Sestkārt, DAN ir noteiktas tiesības uz datu pārnesamību, dodot personām iespēju saņemt savus personas datus strukturētā, plaši izmantotā un mašīnlasāmā formātā un nodot šos datus citam pārzinim ([126]). Šādas tiesības piemēro, ja apstrādi veic ar automatizētiem līdzekļiem, pamatojoties uz personas piekrišanu, vai lai izpildītu līgumu ar fizisku personu vai tās interesēs ([127]).

(51) Visbeidzot, saskaņā ar DAN personām ir tiesības netikt pakļautām automatizētai lēmumu pieņemšanai, proti, lēmumiem, kas balstīti tikai uz automatizētu apstrādi, tostarp profilēšanai, kas rada personai tiesiskas sekas vai būtiski ietekmē viņu līdzīgā veidā ([128]). DAN ir noteikts, ka automatizēta lēmumu pieņemšana var notikt, ja tās pamatā ir datu subjekta nepārprotama piekrišana vai ja tas ir nepieciešams, lai noslēgtu vai izpildītu līgumu ar fizisku personu, un šādā gadījumā pārzinim ir jāveic piemēroti aizsardzības pasākumi, piemēram, nodrošinot tiesības panākt cilvēka iejaukšanos, paust personas viedokli un apstrīdēt lēmumu ([129]). Automatizētu lēmumu pieņemšanu var atļaut arī ar tiesību aktu, ja tajā ir paredzēti piemēroti pasākumi, lai aizsargātu personu tiesības ([130]). Ja pārzinis izmanto automatizētu lēmumu pieņemšanu, tostarp profilēšanu, viņam par to proaktīvi jāinformē persona, pildot savus pārredzamības pienākumus, un jāsniedz jēgpilna informācija par attiecīgo loģiku, kā arī par šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu ([131]). Tāda pati informācija jāsniedz pēc pieprasījuma ([132]).

([120]) DAN 3. panta 1. punkta c) apakšpunkts.
([121]) DAN 21. panta 1. punkts.
([122]) DAN 21. panta 2. punkts.
([123]) Ja EPO ir juridisks pienākums apstrādāt personas datus saistībā ar patentu piešķiršanas procedūru, t. i., saskaņā ar EPK un *PCT*, personas nevar iebilst pret apstrādi, sk. *PGP* lēmuma pielikuma 28. punktu. Ja personas datus apstrādā zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos, datu subjektiem ir tiesības, pamatojoties uz iemesliem, kas saistīti ar viņu īpašo situāciju, iebilst pret personas datu apstrādi, ja vien apstrāde nav nepieciešama, lai izpildītu uzdevumu, ko veic, likumīgi īstenojot pārzinim piešķirtās oficiālās pilnvaras, kas ietver apstrādi, kura nepieciešama Iestādes pārvaldībai un darbībai (DAN 23. panta 4. punkts).
([124]) DAN 23. panta 2. punkts.
([125]) DAN 23. panta 1. punkts.
([126]) DAN 22. panta 1. punkts.
([127]) Tā kā personas datu apstrāde patentu piešķiršanas procedūras kontekstā nav balstīta ne uz vienu no šiem pamatiem, tiesības uz datu pārnesamību šādā kontekstā nav piemērojamas, sk. *PGP* lēmuma pielikuma 29.–30. punktu.
([128]) DAN 24. panta 1. punkts. DAN 3. panta 1. punkta d) apakšpunktā profilēšana tiek definēta kā jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos.
([129]) DAN 24. panta 3. punkts.
([130]) DAN 24. panta 2. punkta b) apakšpunkts.
([131]) Sk. DAN 16. panta 2. punkta f) apakšpunktu un 17. panta 2. punkta f) apakšpunktu.
([132]) DAN 18. panta 1. punkta h) apakšpunkts.

2.4.6.2. *Personas tiesību ierobežojumi*

(52) Līdzīgi kā Regulas (ES) 2016/679 23. pantā un Regulas (ES) 2018/1725 25. pantā DAN 25. pantā ir noteikts, ka konkrētas EPO tiesiskā regulējuma tiesību normas var ierobežot 43.–51. apsvērumā minēto tiesību piemērošanu ([133]) (t. i., ierobežot to piemērošanu uz laiku) ([134]), ja šāds ierobežojums atbilst pamattiesību ([135]) un pamatbrīvību būtībai un ir nepieciešams un samērīgs konkrētu nolūku aizsardzībai demokrātiskā sabiedrībā ([136]). Turklāt ierobežojums ir jāparedz "skaidrās un precīzās" tiesību normās, kuru mērķis ir radīt tiesiskas sekas datu subjektiem un kuras ir jāpieņem vismaz Priekšsēdētāja līmenī ([137]). Šādos noteikumos jo īpaši ir jānosaka apstrādes mērķis, ierobežojuma darbības joma, aizsardzības pasākumi ļaunprātīgas izmantošanas novēršanai un glabāšanas termiņi, kā arī piemērojamie aizsardzības pasākumi ([138]).

(53) Pašlaik vienīgais juridiskais instruments, kas paredz individuālo tiesību ierobežojumus, ir 420. apkārtraksts (juridiski saistošs instruments, ko pieņēmis Priekšsēdētājs). Tajā ir precizēts, kā un ar kādiem nosacījumiem pārzinis var piemērot ierobežojumus, un izsmeļoši noteikti konkrētie gadījumi, kādos tiesības var ierobežot, un ar kādiem mērķiem ([139]). Konkrēti tajā ir paredzēts, ka EPO var ierobežot personas tiesības dažu konkrētu mērķu sasniegšanai: a) un b) risinot izmeklēšanas vai disciplinārlietas attiecībā uz saviem darbiniekiem ([140]); c) saistībā ar strīdu iekšēju izšķiršanu vai juridisku prasību celšanu, īstenošanu vai aizstāvību, tostarp šķīrējtiesā, lai saglabātu konfidenciālu informāciju un dokumentus, kas iegūti no pusēm, personām, kas iestājušās lietā, vai citiem likumiskiem avotiem; d) apstrādājot veselības datus medicīniskajās procedūrās un lietās, bet tikai lai aizsargātu personu tiesības ([141]); e) un f) veicot iekšējās revīzijas un pārbaudes (pēdējās veic DAS); g) IT incidentu pārvaldības un fiziskās drošības incidentu ziņojumu vajadzībām; h) sniedzot palīdzību kompetentām valsts iestādēm vai to saņemot, tostarp no EPO līgumslēdzējām valstīm un starptautiskām organizācijām, vai sadarbojoties ar tām saistībā ar darbībām, kas noteiktas attiecīgajos pakalpojumu līmeņa nolīgumos, saprašanās memorandos un sadarbības nolīgumos, vai nu pēc to pieprasījuma, vai pēc Iestādes iniciatīvas ([142]).

([133]) Izņemot tiesības iebilst, attiecībā uz kurām 420. apkārtrakstā nav paredzēti nekādi ierobežojumi, sk. 3. panta 3. punktu. Turklāt saskaņā ar 420. apkārtraksta 9. pantu EPO var ierobežot personas informēšanu par datu aizsardzības pārkāpumu.

([134]) Sk. ierobežojumu definīciju 420. apkārtraksta 2. pantā.

([135]) Ierobežojumi, kas ir tik plaši un iedarbīgi, ka faktiski atņem pamattiesībām jebkādu jēgu un neļauj indivīdam tās izmantot, nav attaisnojami, sk. 420. apkārtraksta 4. panta 3. punktu.

([136]) Respektīvi, EPO drošība, līgumslēdzēju valstu sabiedrības drošība vai aizsardzība; noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana un saukšana pie atbildības par tiem vai krimināl sodu izpilde, tostarp aizsardzība pret sabiedriskās drošības apdraudējumiem un to novēršana; citas būtiskas EPO intereses, kas saistītas ar tās pamatuzdevumu, vai saistības, kas izriet no pienākuma sadarboties ar līgumslēdzējām valstīm, tostarp monetārie, budžeta un nodokļu jautājumi, sabiedrības veselība un sociālais nodrošinājums; Iestādes, tostarp tās elektronisko sakaru tīklu, iekšējā drošība; tiesas un tiesām pielīdzināmu iestāžu neatkarība, kā arī tiesas un tiesai pielīdzināmu procedūru aizsardzība; reglamentētu profesiju ētikas kodeksu pārkāpumu novēršana, izmeklēšana, atklāšana un sodīšana par tiem; uzraudzības, pārbaudes vai regulatīvo funkciju, kas – pat ja tikai epizodiski – ir saistīta ar oficiālu pilnvaru īstenošanu; datu subjekta vai citu personu tiesību un brīvību aizsardzība un civilprasību izpilde (DAN 25. panta 1. punkts).

([137]) DAN 25. panta 3. punkts.

([138]) DAN 25. panta 2. punkts.

([139]) 420. apkārtraksta 1. pants.

([140]) 420. apkārtraksta 4. panta 1. punkta a) un b) apakšpunkts.

([141]) Tas attiecas tikai uz EPO darbinieku veselības datu apstrādi (un tieši neattiecas uz konstatējumu par aizsardzības līmeņa pietiekamību par tādu datu apstrādi, kuri nosūtīti no pārziņa vai apstrādātāja, uz kuru attiecas VDAR). 420. apkārtraksta 8. pantā ir sīkāk paskaidrots, kā var piemērot ierobežojumus attiecībā uz tiesībām piekļūt medicīniskajiem datiem/datnēm. Konkrēti, tajā ir precizēts, ka šādu ierobežojumu var piemērot tikai tiesībām tieši piekļūt saviem personas medicīniskajiem datiem un/vai psiholoģiska vai psihiatriska rakstura lietas materiāliem, ko apstrādā Iestāde, bet tikai tad, ja piekļuve šiem datiem var nelabvēlīgi ietekmēt un radīt tūlītējus draudus datu subjekta vai citu personu dzīvībai un veselībai.

([142]) 420. apkārtraksta 4. panta 1. punkts. Šis noteikums būtībā attiecas tikai uz EPO darbinieku personas datiem. Tas attiecas uz gadījumiem, kad EPO ir jāsadarbojas ar līgumslēdzēju valstu iestādēm saskaņā ar EPK 131. pantu (kas reglamentē sadarbību starp EPO un līgumslēdzēju valstu tiesām izmeklēšanā/procesos saistībā ar patentu piešķiršanu) un tās Protokola par privilēģijām un imunitāti 20. panta 1. punktu (sk. arī 95. punktu). Tas var attiekties, piemēram, uz gadījumiem, kad EPO darbiniekiem prasa liecināt līgumslēdzējas valsts tiesā saistībā ar valsts krimināl procesu vai ja EPO tiek lūgts sniegt informāciju par sava personāla atalgojumu civilprocesā (ģimenes tiesībās) utt.

(54) Tas, vai konkrētā gadījumā ierobežojumu var piemērot, ir jānosaka pārzinim individuālos gadījumos, ņemot vērā attiecīgos apstākļus ([143]). Lemjot par ierobežojuma piemērošanu vai nepiemērošanu, pārzinim vispirms ir jānovērtē tā nepieciešamība un samērīgums konkrētajā gadījumā, iesaistot DAS ([144]). Minētais novērtējums ietver iespējamo risku datu subjekta tiesībām un brīvībām izsvēršanu pretstatā citu datu subjektu riskiem un brīvībām un riskiem, kas var traucēt apstrādes darbības nolūkam un iznākumam ([145]). Ierobežojumi ir jādokumentē: jāreģistrē ierobežoto tiesību novērtējums, ierobežojuma ilgums, tā iemesli un pamats ([146]). Turklāt, kamēr tiek piemērots ierobežojums, ir jāievieš atbilstoši tehniskie un organizatoriskie pasākumi ([147]). Jebkuru ierobežojumu var piemērot tikai tik ilgi, kamēr pastāv ierobežojuma iemesli ([148]). Ja tiesības tiek ierobežotas, pārzinim jāinformē attiecīgā persona par galvenajiem iemesliem un tiesībām iesniegt sūdzību ([149]).

2.4.6.3. *Īpaši noteikumi saistībā ar patentu piešķiršanas procedūru*

(55) EPO dibināšanas līgumā (proti, EPK), *PCT* noteikumos un saskaņā ar tiem piemērojamajos noteikumos (kas visi ir EPO primārie tiesību akti) ir ietvertas konkrētas īpašas prasības saistībā ar patentu piešķiršanas procedūru, kas var ietekmēt noteiktu tiesību īstenošanu saskaņā ar DAN ([150]). *PGP* lēmumā ir sniegts pārskats par minētajām primāro tiesību aktu prasībām, paskaidrots, kā šajā kontekstā var īstenot datu subjektu tiesības, un skaidri noteikti iespējamie izņēmumi ([151]). 420. apkārtrakstā ir noteikts, ka tajos noteikumos, kas var ierobežot datu aizsardzības tiesību piemērošanu, ir skaidri jānorāda jebkura atbrīvojuma darbības joma un tādējādi jālīdzsvaro dažādās iesaistītās intereses ([152]).

(56) Pirmkārt, saskaņā ar EPK 127. pantu Iestādei ir pienākums uzturēt Eiropas Patentu reģistru, kur tiek publicēti konkrēti juridiski definēti personas dati. Saskaņā ar primārajiem tiesību aktiem patentu pieteikumi ir jāpublicē patentu piešķiršanas procedūras laikā, parasti iespējami drīz pēc astoņpadsmit mēnešu termiņa beigām no pieteikuma iesniegšanas dienas. EPK paredz, ka šādos patentu pieteikumos iekļautajiem personas datiem var piekļūt, vai nu pārbaudot lietas materiālus, vai pārbaudot reģistru ([153]). Pirms publicēšanas patentu pieteikumi nav pieejami pārbaudei bez pieteikuma iesniedzēja nepārprotamas piekrišanas. Līdzīgi noteikumi ir paredzēti *PCT* ([154]).

([143]) 420. apkārtraksta 2. pants.

([144]) DAN 25. panta 3. punkta a) apakšpunkts. Sk. arī 420. apkārtraksta 6. pantu.

([145]) 420. apkārtraksta 5. panta 5. punkts.

([146]) 420. apkārtraksta 4. panta 4. punkts. Šie ieraksti pēc pieprasījuma ir jādara pieejami DAP (420. apkārtraksta 4. panta 7. punkts).

([147]) Tādi kā, piemēram, droša glabāšana, droša elektroniskā vide, kas novērš nelikumīgu un nejaušu piekļuvi elektroniskajiem datiem vai to nosūtīšanu nepilnvarotām personām, un ierobežojumu uzraudzība un to piemērošanas periodiska pārskatīšana, sk. 420. apkārtraksta 5. panta 2. punktu.

([148]) 420. apkārtraksta 4. panta 5. punkts un 5. panta 3. punkts.

([149]) DAN 25. panta 3. punkta b) apakšpunkts. Šo informāciju var atlikt, izlaist vai atteikt, ja ar to tiktu atcelta ierobežojuma ietekme, sk. DAN 25. panta 4. punktu. Šo papildu ierobežojumu var piemērot tikai pienācīgi pamatotos gadījumos un tik ilgi, cik tas ir nepieciešams un ir samērīgi (420. apkārtraksta 7. panta 4. punkts). Šāda ierobežojuma pamatojums ir regulāri atkārtoti jāizvērtē. Papildus īpašajai prasībai informēt personas par viņu tiesību ierobežojumiem EPO savā iekštīklā un/vai tīmekļa vietnē ir jāsniedz vispārīga informācija par darbībām, kas var ietvert tiesību ierobežojumus (420. apkārtraksta 7. panta 1. punkts).

([150]) 420. apkārtraksta 2. pants (EPO tiesību normas).

([151]) *PGP* lēmuma 1. pants un pielikums.

([152]) 420. apkārtraksta 2. pants.

([153]) *PGP* lēmuma pielikuma C.13. un C.14. punkts un EPK 128. pants. Noteiktas lietas daļas ir izslēgtas no lietu pārbaudes saskaņā ar EPK īstenošanas noteikumu 128. panta 4. punktu un 144. pantu un EPO Priekšsēdētāja 2007. gada 12. jūlija lēmumu par dokumentiem, kas izslēgti no lietu pārbaudes (Īpašais izdevums Nr. 3, OV EPO 2007, J.3). Izslēgtās daļas ir šādas: dokumenti, kas saistīti ar apelācijas padomju vai paplašinātās apelācijas padomes locekļu izslēgšanu vai iebildumiem pret tiem; lēmumu un paziņojumu projekti, kā arī visi citi dokumenti, ko izmanto lēmumu un paziņojumu sagatavošanai un kas netiek darīti zināmi pusēm; izgudrotāja vārds, ja viņš ir atteicies no savām tiesībām tikt pieminētam, un jebkurš cits dokuments, ko Eiropas Patentu iestādes Priekšsēdētājs nevar pārbaudīt, pamatojoties uz to, ka šāda pārbaude nekalpotu sabiedrības informēšanai par Eiropas patenta pieteikumu vai Eiropas patentu, piemēram: medicīniskās izziņas; lūgumi izslēgt no lietas pārbaudes un ar to saistītās sarakstes; informācija, kuras publicēšana kaitē likumīgām personiskām vai ekonomiskām interesēm un neietver informāciju, kas attiecas uz pieteikumu, patentu vai piešķiršanas procedūru.

([154]) Sk. 3. pantu EPO Priekšsēdētāja 2019. gada 20. februāra lēmumā par to dokumentu pārbaudi tiešsaistē, kuri atrodas EPO kā saņēmējas iestādes, Starptautiskās meklēšanas iestādes vai iestādes, kas norādīta papildu meklēšanai, rīcībā (OV Eiropas Patentu iestāde 2019, A17). Šajā sakarā sk. *PCT* 30. pantu par publisku piekļuvi lietām, kā arī PCT 94. un 48. pantu. EPO atsaucas uz šiem noteikumiem, kad tā darbojas kā kompetentā iestāde vai struktūra atbilstoši PCT saskaņā ar EPK 151.–153. pantu.

(57) Otrkārt, EPK īpaši reglamentē iespēju panākt izmaiņas informācijā, ko izmanto saistībā ar patentu piešķiršanas procedūru ([155]). Konkrēti EPK ir paredzēta tikai iespēja panākt kļūdu labošanu EPO iesniegtajos dokumentos ([156]), kļūdu labošanu lēmumos ([157]), tulkojumu labošanu ([158]) un izgudrotāja vārda labošanu ([159]). Tāpēc patentu piešķiršanas procedūrā izmantotajos dokumentos iekļauto personas datu labošanu arī var panākt tikai šajos gadījumos. Tas pats attiecas uz iespēju panākt datu apstrādes ierobežojumu ([160]).

(58) Treškārt, EPK ir noteiktas īpašas saglabāšanas un publicēšanas prasības attiecībā uz dažiem dokumentiem, ko izmanto patentu piešķiršanas procedūrā, un tas ietekmē iespēju panākt tajos ietvertās informācijas, tostarp personas datu, dzēšanu ([161]). Konkrēti, Eiropas Patentu biļetenā publicētie patentu pieteikumi un patentu informācija ir jāsaglabā un jāsaglabā publiski pieejama ([162]). Tādējādi šajos dokumentos ietverto personas datu dzēšana būtu pretrunā EPO pamata juridiskajām saistībām (EPK 129. panta a) punkts), un to nevar panākt. Citas datnes EPO ir jāglabā EPK noteikto laikposmu, kas principā ir pieci gadi ([163]). Kamēr šis termiņš nav beidzies, šajās datnēs ietvertās informācijas (tostarp personas datu) dzēšanu nevar panākt.

(59) Tādējādi, īpaši ņemot vērā to ierobežoto darbības jomu un piemērošanas nosacījumus, var uzskatīt, ka no 55. līdz 58. apsvērumā minētajiem noteikumiem izrietošie tiesību izmantošanas ierobežojumi aprobežojas ar to, kas ir nepieciešams un samērīgs, lai nodrošinātu pareizu patenta piešķiršanas procedūras darbību, kā tas nepieciešams sabiedrības interesēs EPO oficiālo uzdevumu izpildei. Ciktāl EPK un *PCT* konkrēti nereglamentē datu aizsardzības tiesību īstenošanu, proti, visos citos scenārijos, kas nav aprakstīti 55.–58. apsvērumā, DAN prasības ir piemērojamas pilnībā.

2.4.7. ***Tālāka pārsūtīšana***

(60) Aizsardzības līmeni, kāds piešķirts personas datiem, kurus no Savienības nosūta EPO, nedrīkst samazināt šādu datu tālāka nosūtīšana saņēmējiem trešā valstī vai citā starptautiskā organizācijā.

(61) DAN ir nošķirta "personas datu nosūtīšana" (t. i., EPO datu kopīgošana ar līgumslēdzējām valstīm) un "personas datu pārsūtīšana" (EPO veiktā datu kopīgošana ar jebkuru citu personu vai struktūru ārpus EPO) ([164]).

2.4.7.1. *Datu pārsūtīšana*

(62) Pirmkārt, DAN ir paredzēts, ka datu nosūtīšana EPO līgumslēdzējas valsts intelektuālā īpašuma birojam var notikt, ja dati ir nepieciešami a) saņēmēja kompetences īstenošanai vai oficiālu pilnvaru īstenošanai un b) nosūtīšana ir nepieciešama EPO oficiālo uzdevumu/funkciju izpildei ([165]). Šī nosūtīšana notiek EPK un *PCT* paredzētās patentu piešķiršanas procedūras ietvaros ([166]).

([155]) Veicot labojumus vai precizējumus saskaņā ar šiem noteikumiem, var tikt atjaunināti ieraksti Eiropas Patentu reģistrā un Eiropas Patentu biļetenā, kā arī pieteikuma vai patenta publikācijas. Tomēr tie ar atpakaļejošu spēku nemaina lietas saturu (kas arī turpmāk ietver visus pušu iesniegumus un EPO paziņojumus un lēmumus). Arī agrākās publikācijas netiek ne atsauktas, ne dzēstas (*PGP* lēmuma pielikuma C.19. punkts). Tas attiecas arī uz *PCT* 19. un 34. pantu, ja EPO darbojas kā kompetentā struktūra/iestāde, pamatojoties uz EPK 151.–153. pantu.

([156]) EPK īstenošanas noteikumu 139. pants.

([157]) EPK īstenošanas noteikumu 140. pants. EPO lēmumos drīkst labot tikai valodas kļūdas, transkripcijas kļūdas un acīmredzamas kļūdas.

([158]) EPK 14. panta 2. punkta otrais teikums.

([159]) EPK īstenošanas noteikumu 21. pants. Nepareizu izgudrotāja vārdu var labot pēc pieprasījuma un tikai ar kļūdaini norādītās personas piekrišanu un, ja šādu pieprasījumu iesniedz trešā persona, ar patenta pieteikuma iesniedzēja vai īpašnieka piekrišanu.

([160]) *PGP* lēmuma pielikuma C.25. punkts.

([161]) *PGP* lēmuma pielikuma C.22. un C.23. punkts.

([162]) EPK 129. pants.

([163]) EPK īstenošanas noteikumu 147. panta 4. un 5. punkts.

([164]) DAN 3. panta 1. punkta s) un t) apakšpunkts.

([165]) DAN 8. panta 2. punkts.

([166]) Sk. jo īpaši EPK 130., 131. un 135. pantu, kā arī attiecīgos EPK īstenošanas noteikumus (piemēram, 148.–150. pantu). Sk. arī *PCT* 12., 18., 20. un 36. pantu, kā arī īstenošanas noteikumu 22., 23., 23.a, 44., 47. un 71. pantu.

(63) Otrkārt, DAN ļauj nosūtīt datus EPO līgumslēdzējas valsts publiskai iestādei ([167]), ja dati ir nepieciešami šīs publiskās iestādes uzdevumu izpildei un nosūtīšana ir saderīga ar EPO uzdevumiem un darbību ([168]). Šāda nosūtīšana netiek konkrēti prasīta saskaņā ar EPK vai citiem juridiskiem instrumentiem, kas reglamentē patentu piešķiršanas procedūru, tomēr tā var būt nepieciešama EPO uzdevumu izpildei, piemēram, EPO sadarbībai ar līgumslēdzējām valstīm konsultāciju procesā, ekspertu norīkošanai un izvietošanai vai informācijas sniegšanai par EPO darbiniekiem nolūkā noteikt sociālos pabalstus, nodokļu prasības utt.

(64) DAS ir sagatavojis paraugklauzulas, kas jāiekļauj saprašanās memorandos, kuri reglamentē šādu 62. un 63. apsvērumā aprakstītu nosūtīšanu, kas tostarp paredz datu aizsardzības principus, ierobežo turpmāku apstrādi tikai savietojamos nolūkos, paredz datu subjektu tiesības, kā arī pienākumus attiecībā uz datu drošību un datu aizsardzības pārkāpumiem un neatkarīgu uzraudzību ([169]).

(65) Abos 62. un 63. apsvērumā aprakstītajos scenārijos saņēmējam saskaņā ar DAN ir jāsniedz pierādījumi, ka dati ir jānosūta konkrētam mērķim, kas izriet no EPO saistībām sadarboties ar līgumslēdzēju valsti vai valstīm ([170]). Pārzinim attiecībā uz katru nosūtīšanu jāspēj pierādīt, ka šāda nosūtīšana ir nepieciešama un samērīga ar konkrēto nolūku, kādā tā tiek veikta ([171]). Datu pārsūtīšanai jānotiek tā, lai nodrošinātu, ka tiek saglabāts DAN noteiktais aizsardzības līmenis ([172]). Saskaņā ar DAS sniegtajiem norādījumiem tas nozīmē, ka tiek nodrošināti atbilstoši aizsardzības pasākumi, tai skaitā kopīgojamie dati ir jāsamazina līdz minimumam un jāaprobežojas ar to, kas ir pienācīgs, atbilstošs un absolūti nepieciešams šā mērķa sasniegšanai ([173]). Ja ir pamats uzskatīt, ka var tikt skartas attiecīgās personas likumīgās intereses, pārzinim pēc dažādo interešu izsvēršanas ir jāpierāda, ka personas datu nosūtīšana šim konkrētajam nolūkam ir samērīga ([174]).

(66) Attiecībā uz šiem diviem scenārijiem ir svarīgi arī norādīt, ka visas EPO līgumslēdzējas valstis ir Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas līgumslēdzējas puses, uz kurām attiecas Eiropas Cilvēktiesību tiesas jurisdikcija, kā arī Eiropas Padomes Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (ETS Nr. 108) puses.

(67) Visbeidzot, DAN atļauj nosūtīt datus apstrādātājam, kas atrodas Eiropas Ekonomikas zonā (EEZ), ar nosacījumu, ka tiek nodrošināta atbilstība DAN noteiktajām prasībām attiecībā uz apstrādātāju iesaistīšanu ([175]).

2.4.7.2. *Datu pārsūtīšana*

(68) Personas datu kopīgošana ar jebkuru struktūru ārpus EPO, kas nav EPO līgumslēdzēju valstu publiska iestāde vai valsts intelektuālā īpašuma birojs, vai apstrādātājs EEZ, tiek uzskatīta par personas datu "pārsūtīšanu", kurai jāpiemēro konkrētas DAN prasības ([176]). Minētās prasības attiecas, piemēram, uz datu kopīgošanu ar apstrādātājiem ārpus EEZ, pārziņiem, kas atrodas līgumslēdzējās valstīs vai ārpus tām, valsts iestādēm valstīs, kas nav līgumslēdzējas valstis, un citām starptautiskām organizācijām. DAN ir vispārīgi noteikts, ka, nosūtot datus trešām personām, netiek

([167]) Piemēram, valsts vai vietējā iestāde, kā arī cits publisko tiesību subjekts, kā slimnīca vai universitāte.
([168]) DAN 8. panta 1. punkts.
([169]) Pārskats par prasību attiecībā uz EPO datu aizsardzības paraugklauzulu saprašanās memorandos, pieejams tīmekļa vietnē https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-template-data-protection-clause-for-mous.pdf.
([170]) DAN 8. panta 3. punkts.
([171]) DAN 8. panta 4. punkts.
([172]) Paskaidrojošais dokuments "EPO personas datu nosūtīšana un pārsūtīšana" (nosūtīšanas un pārsūtīšanas dokuments), pieejams tīmekļa vietnē https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, 4. lpp. Konkrēti, sk. "EPO DAN [...] nosaka vispārēju pienācīgas aizsardzības principu, kas jo īpaši piemērojams starptautiskai datu plūsmai."
([173]) Nosūtīšanas un pārsūtīšanas dokuments, pieejams 12. zemsvītras piezīmē.
([174]) DAN 8. panta 3. punkts.
([175]) DAN 8. panta 1., 2. un 5. punkts.
([176]) DAN 9. panta 1. punkts.

apdraudēts aizsardzības līmenis, ko personām garantē EPO ([177]). Saskaņā ar DAS norādījumiem uz trešo valsti vai starptautisko organizāciju pārsūtītajiem personas datiem piešķirtajai aizsardzībai būtībā ir jābūt "līdzvērtīgai aizsardzībai, kas garantēta DAN" ([178]).

(69) Saskaņā ar DAN personas datu pārsūtīšana ārpus EPO var notikt tikai tad, ja valsts, kurā atrodas saņēmējs, vai starptautiskā organizācija nodrošina pienācīgu aizsardzības līmeni un ja pārsūtīšana tiek veikta tikai tāpēc, lai EPO varētu veikt uzdevumus, kas ir tās kompetencē ([179]). Lēmumu par aizsardzības līmeņa pietiekamību pieņem Priekšsēdētājs ([180]), kurš šaubu gadījumā apspriežas ar DAS un DAP ([181]). DAS ir izstrādājis "pietiekamības atsauces", nosakot kritērijus lēmumiem par aizsardzības līmeņa pietiekamību ([182]). Konkrēti trešās valsts vai starptautiskās organizācijas tiesiskajā regulējumā jāparedz galvenie datu aizsardzības principi, datu subjektu tiesības, noteikumi par tālāku pārsūtīšanu, procesuālie un izpildes mehānismi un personu tiesiskā aizsardzība. Ja Priekšsēdētājs pieņem lēmumu par aizsardzības līmeņa pietiekamību, pārsūtīšanu var veikt, neveicot papildu aizsardzības pasākumus ([183]). EPO pašlaik uzskata, ka dalībvalstis, kā arī Norvēģija, Islande, Lihtenšteina, visas valstis, uz kurām attiecas Komisijas un Savienības iestāžu un struktūru lēmums par aizsardzības līmeņa pietiekamību ([184]), nodrošina pienācīgu aizsardzības līmeni ([185]).

(70) Saskaņā ar DAN, ja nav lēmuma par aizsardzības līmeņa pietiekamību, pārzinis vai apstrādātājs var nosūtīt personas datus saņēmējiem ārpus EPO tikai tad, ja pārzinis vai apstrādātājs ir veicis atbilstošus aizsardzības pasākumus un ar nosacījumu, ka datu subjektiem ir pieejamas īstenojamas datu subjektu tiesības un efektīvi tiesiskās aizsardzības līdzekļi ([186]). Šādus atbilstošus aizsardzības pasākumus var iekļaut administratīvajās vienošanās ar valsts iestādēm vai starptautiskām organizācijām, līguma klauzulās (pēc apspriešanās ar DAP) ([187]) vai sertifikācijas mehānismos ([188]). DAS ir izstrādājis administratīvajās vienošanās iekļaujamo noteikumu paraugu ([189]). Ir pieejams arī datu aizsardzības nolīguma paraugs datu pārsūtīšanai apstrādātājiem ([190]). Saskaņā ar DAS norādījumiem EPO ir jānovērtē, vai datu saņēmējam būtu liegts izpildīt savus pienākumus saskaņā ar pārsūtīšanas instrumentu uz to attiecināmā tiesiskā regulējuma dēļ, un vajadzības gadījumā jāievieš papildu pasākumi ([191]). Lai veiktu šo novērtējumu, DAS savos EPO paskaidrojumos par personas datu nosūtīšanu un pārsūtīšanu iesaka ņemt vērā attiecīgos EDAK un Eiropas Datu aizsardzības uzraudzītāja norādījumus ([192]).

(71) Saskaņā ar DAN attiecībā uz datu pārsūtīšanu valstīm vai organizācijām, uz kurām attiecas lēmums par aizsardzības līmeņa pietiekamību, kā arī attiecībā uz datu pārsūtīšanu, pamatojoties uz atbilstošiem aizsardzības pasākumiem, EPO ir jāpierāda katras nosūtīšanas nepieciešamība un samērīgums apstrādes nolūkā ([193]). Turklāt, ja ir pamats uzskatīt, ka varētu tikt aizskartas datu subjektu likumīgās intereses, EPO pēc dažādo iesaistīto interešu izsvēršanas ir jāpierāda, ka pārsūtīšana ir samērīga ([194]). Turklāt ir jānodrošina (izmantojot līgumiskus aizsardzības pasākumus), ka

([177]) DAN 9. panta 1. punkts.
([178]) Nosūtīšanas un pārsūtīšanas dokuments, 11. lpp. un 8. zemsvītras piezīme. "Trešā valsts" DAN ir definēta kā valsts, kas nav EPK līgumslēdzēja valsts, sk. DAN 3. panta 1. punkta u) apakšpunktu.
([179]) DAN 9. panta 2. punkts.
([180]) Sk. DAN 1. panta 2. punkta a) apakšpunktu kopsakarā ar EPK 10. panta 2. punkta a) apakšpunktu un DAN 9. panta 2. punktu.
([181]) DAN 9. panta 3. punkts.
([182]) EPO pietiekamības atsauces dokumenta izklāsts pieejams tīmekļa vietnē https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-adequacy-referential-methodology.pdf.
([183]) Nosūtīšanas un pārsūtīšanas dokumenta 49. zemsvītras piezīme.
([184]) Izņemot ES un ASV datu privātuma regulējumu.
([185]) Sk. Eiropas Patentu iestādes Priekšsēdētāja 2022. gada 17. novembra lēmumu par valstīm un vienībām, kuras uzskata par tādām, kas nodrošina personas datu pienācīgu aizsardzību, pieejams tīmekļa vietnē https://www.epo.org/en/legal/official-journal/2022/12/a111.html.
([186]) DAN 9. panta 4. un 5. punkts.
([187]) Šajā sakarā DAS norādījumos ir atsauce uz Eiropas Komisijas pieņemtajām līguma standartklauzulām, kas sniedz labu pārskatu par iekļaujamajiem aizsardzības pasākumiem, sk. nosūtīšanas un pārsūtīšanas dokumentu, 8. lpp.
([188]) DAN 9. panta 5. punkts. Sk. arī nosūtīšanas un pārsūtīšanas dokumentu, 8. lpp.
([189]) Pārskats par prasībām attiecībā uz EPO administratīvo vienošanos paraugiem, pieejams tīmekļa vietnē https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-epo's-administrative-arrangements-modules.pdf.
([190]) Sk. EPO vispārējo līguma noteikumu E pielikumu, pieejams https://link.epo.org/web/general_conditions_of_contract_en.pdf.
([191]) Nosūtīšanas un pārsūtīšanas dokuments, 9. lpp.
([192]) Nosūtīšanas un pārsūtīšanas dokuments, 9. lpp.
([193]) DAN 9. panta 6. punkts. Ja ir pamats uzskatīt, ka datu subjekta likumīgās intereses varētu tikt aizskartas, pārzinim, izvērtējot dažādās konkurējošās intereses, ir jāpierāda, ka nosūtīšana konkrētajā nolūkā ir samērīga.
([194]) DAN 9. panta 6. punkts.

saņēmējs var apstrādāt vai izmantot datus tikai tiem mērķiem, kādiem tie tika pārsūtīti, un dati ir jādzēš, tiklīdz mērķis ir sasniegts ([195]).

(72) Saskaņā ar DAN, ja lēmuma par aizsardzības līmeņa pietiekamību vai atbilstošu aizsardzības pasākumu nav, personas datu pārsūtīšana ārpus EPO ir pieļaujama "tikai izņēmuma kārtā", ja ir piemērojama tā sauktā "atkāpe" ar līdzīgiem nosacījumiem kā attiecīgajos Savienības datu aizsardzības tiesību aktu noteikumos ([196]). Tā tas ir gadījumā, ja a) datu subjekts ir skaidri piekritis pārsūtīšanai ([197]), b) un c) pārsūtīšana ir neregulāra un nepieciešama, lai izpildītu līgumu ar datu subjektu vai tā interesēs (vai lai pēc datu subjekta pieprasījuma īstenotu pasākumus pirms līguma noslēgšanas) ([198]), d) pārsūtīšana ir vajadzīga uzdevuma izpildei, kas saistīta ar EPO oficiālo darbību veikšanu, vai pārzinim oficiāli piešķirto pilnvaru īstenošanai ([199]), e) pārsūtīšana ir neregulāra un vajadzīga, lai celtu, īstenotu vai aizstāvētu juridiskas prasības ([200]), f) pārsūtīšana ir vajadzīga, lai aizsargātu personas vitālas intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot nepārprotamu piekrišanu ([201]), vai g) pārsūtīšanu izdara no reģistra, kurš ir paredzēts, lai sniegtu informāciju sabiedrībai, un kurš ir pieejams, lai informāciju gūtu gan plaša sabiedrība, gan jebkura persona, kura var pierādīt likumīgu ieinteresētību, ciktāl par informācijas pieejamību izvirzītie nosacījumi konkrētajā gadījumā tiek izpildīti ([202]). Pēc būtības un saskaņā ar DAS norādījumiem uz šīm atkāpēm nevar atsaukties, lai veiktu sistemātisku un regulāru pārsūtīšanu ([203]).

(73) Visbeidzot, attiecībā uz konkrētu kategoriju datu pārsūtīšanu valstīm vai organizācijām, uz kurām neattiecas lēmums par aizsardzības līmeņa pietiekamību, Priekšsēdētājs var vēl vairāk ierobežot šādu pārsūtīšanu svarīgu iemeslu dēļ, kas saistīti ar Iestādei piešķirto oficiālo pilnvaru likumīgu īstenošanu ([204]). Līdz šim Priekšsēdētājs šīs pilnvaras nav izmantojis.

2.4.8. ***Pārskatatbildība***

(74) Saskaņā ar pārskatatbildības principu vienībām, kas apstrādā datus, ir jāievieš atbilstoši tehniskie un organizatoriskie pasākumi, lai tās efektīvi izpildītu savus datu aizsardzības pienākumus, un jāspēj pierādīt šādu izpildi, konkrēti – kompetentajai uzraudzības iestādei.

(75) DAN 4. panta 1. punktā ir noteikts vispārējs pārskatatbildības princips, ar kuru tiek noteikts, ka pārzinis ir atbildīgs par DAN ievērošanu un tam ir jāspēj to pierādīt. Konkrēti, pārzinim ir jāveic atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu un spētu pierādīt atbilstību, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, kā arī risku atšķirīgo iespējamību un nopietnību attiecībā uz fizisku personu tiesībām ([205]). Šajā ziņā DAN

([195]) DAN 9. panta 6. punkts.
([196]) Skatīt DAN 10. pantu, kā arī nosūtīšanas un pārsūtīšanas dokumentu, 9.–11. lpp.
([197]) DAN 10. panta 1. punkta a) apakšpunkts. Šajā gadījumā persona ir jāinformē par iespējamiem riskiem, ko rada pienācīga aizsardzības līmeņa un atbilstošu aizsardzības pasākumu trūkums. EPO nevar atsaukties uz šo atkāpi, veicot savas oficiālās darbības (DAN 10. panta 2. punkts).
([198]) DAN 10. panta 1. punkta b) un c) apakšpunkts un 2. punkts. EPO nevar atsaukties uz šīm atkāpēm, veicot savas oficiālās darbības (DAN 10. panta 2. punkts).
([199]) DAN 10. panta 1. punkta d) apakšpunkts. Šādas oficiālas darbības vai pilnvaras ir jānosaka, pamatojoties uz EPK vai citām piemērojamām Eiropas Patentu organizācijas tiesību normām (DAN 10. panta 4. punkts). Tās ietver apstrādi, kas vajadzīga Iestādes vadībai un darbībai vai tādu pienākumu izpildei, kas izriet no EPO pienākuma sadarboties ar līgumslēdzējām valstīm. Pārsūtīšana var notikt, lai izpildītu pienākumus, piemēram, starp Iestādi un valstu struktūrām, nodokļu vai muitas iestādēm, finanšu uzraudzības iestādēm un dienestiem, kas ir kompetenti sociālā nodrošinājuma jautājumos vai sabiedrības veselības jomā, piemēram, kontaktu izsekošanai lipīgu slimību gadījumā (DAN 10. panta 6. punkts).
([200]) DAN 10. panta 1. punkta e) apakšpunkts un 2. punkts.
([201]) DAN 10. panta 1. punkta f) apakšpunkts.
([202]) DAN 10. panta 1. punkta g) apakšpunkts. Šajā gadījumā nevar pārsūtīt pilnīgi visus reģistrā ietvertos personas datus vai veselas datu kategorijas, ja vien to neatļauj Eiropas Patentu organizācijas tiesību normas, un, ja reģistrs ir paredzēts, lai to varētu izmantot personas ar leģitīmu interesi, dati būtu jānosūta tikai pēc šo personu pieprasījuma vai ja šīs personas ir datu saņēmējas, pilnībā ņemot vērā datu subjekta intereses un pamattiesības (DAN 10. panta 2. un 5. punkts).
([203]) Nosūtīšanas un pārsūtīšanas dokuments, 10. lpp.
([204]) Tās, kā minēts iepriekš, ietver apstrādi, kas vajadzīga tās pārvaldībai un darbībai, vai saistībā ar pienākumiem, kas izriet no pienākuma sadarboties ar līgumslēdzējām valstīm. Sk. DAN 10. panta 6. punktu.
([205]) DAN 26. panta 1. punkts.

īsteno arī integrētas privātuma aizsardzības un privātuma pēc noklusējuma principus, pieprasot pārzinim veikt pasākumus, kas paredzēti, lai īstenotu datu aizsardzības principus un nodrošinātu atbilstību DAN, kā arī nodrošināt, ka pēc noklusējuma tiek apstrādāti tikai katram konkrētajam apstrādes nolūkam nepieciešamie personas dati ([206]).

(76) Pārzinim un apstrādātājiem ir jāreģistrē apstrādes darbības, tostarp ietverot informāciju par apstrādes nolūku, apstrādāto datu kategorijām, to saņēmēju kategorijām, kuriem dati tiek izpausti, un personas datu pārsūtīšanu ([207]). Šie reģistra ieraksti principā ir publiski pieejami (ja vien nesatur konfidenciālu informāciju), tiek iekļauti publiski pieejamā datu aizsardzības reģistrā un pēc pieprasījuma ir jādara pieejami DAP ([208]). Katrai operatīvajai vienībai arī jāieceļ vismaz viens datu aizsardzības koordinators (uz atjaunojamu termiņu no viena līdz trim gadiem), kam jāiziet obligāta apmācība datu aizsardzības jomā un jāpalīdz pārzinim pildīt tā pienākumus ([209]).

(77) Visbeidzot, DAN ir paredzēti dažādi instrumenti, kas var palīdzēt pārzinim un apstrādātājiem atbilstības nodrošināšanas centienos. Piemēram, saskaņā ar DAN apstiprināto sertifikācijas mehānismu ievērošana var kalpot par pierādījumu DAN saistību izpildei ([210]). Turklāt noteiktos apstākļos DAN ir prasīts veikt novērtējumu par ietekmi uz datu aizsardzību vai iepriekšēju apspriešanos ar DAS un DAP. Novērtējums par ietekmi uz datu aizsardzību ir vajadzīgs, ja apstrādes veids var radīt augstu risku personas tiesībām un brīvībām ([211]). Tas, piemēram, ir nepieciešams, ja sistemātiski un plaši tiek izvērtēti personiskie aspekti, uz kuriem balstīti automatizēti lēmumi, vai ja tiek veikta īpašu kategoriju datu apstrāde lielā apjomā ([212]). Ja ietekmes novērtējums liecina, ka apstrāde radītu augstu risku personu tiesībām un brīvībām un ka risku nevar mazināt ar saprātīgiem drošības pasākumiem, pārzinim ir jāapspriežas ar DAP ([213]). Ja DAP uzskata, ka plānotā apstrāde būtu DAN pārkāpums, tai ir jāsniedz rakstisks ieteikums ([214]). Vispārīgāk runājot, pārzinim, sagatavojot noteikumus vai darbības dokumentus par individuālo tiesību ierobežojumu īstenošanu, ir jāapspriežas ar DAS ([215]).

2.5. **Pārraudzība un izpilde**

(78) Lai nodrošinātu, ka arī praksē tiek garantēts pietiekams datu aizsardzības līmenis, vajadzētu būt izveidotai neatkarīgai uzraudzības iestādei, kurai uzticētas pilnvaras uzraudzīt un nodrošināt datu aizsardzības noteikumu izpildi. Šai iestādei savi uzdevumi būtu jāveic un pilnvaras jāīsteno pilnīgi neatkarīgi un objektīvi.

(79) EPO tiesiskajā regulējumā divām struktūrām, DAS un DAP, ir uzticēts pārraudzīt, kā EPO ievēro datu aizsardzības noteikumus. Abas struktūras ir izveidotas ar dienesta noteikumu 32.A pantu, savukārt to statuss un pilnvaras ir sīkāk precizētas DAN ([216]). To uzdevumi ir savstarpēji papildinoši un ietver sadarbību, tomēr katra struktūra savās attiecīgajās funkcijās joprojām ir neatkarīga.

([206]) DAN 27. panta 1. un 2. punkts.
([207]) DAN 32. panta 1. un 2. punkts. Saskaņā ar DAN 4. panta 1. punktu pārzinim "apstrādes darbību izstrādē un dokumentēšanā ir jāievēro strukturēta un uz risku balstīta pieeja". Pārzinim arī jāspēj vienmēr pierādīt datu subjektiem, ka, veicot apstrādes darbības, tiek ievērotas dokumentētās saistības un nosacījumi.
([208]) DAN 32. panta 4., 5. un 6. punkts.
([209]) DAN 45. pants.
([210]) DAN 26. panta 3. punkts.
([211]) Attiecībā uz nepieciešamību veikt ietekmes novērtējumu pārzinim ir jākonsultējas ar DAS, kas šaubu gadījumā savukārt var vērsties pie DAP. Sk. DAN 38. panta 1. un 2. punktu.
([212]) DAN 38. panta 4. punkts.
([213]) DAN 38. panta 6. punkts.
([214]) DAN 38. panta 7. un 8. punkts un 39. pants.
([215]) DAN 40. panta 2. punkts.
([216]) Dienesta noteikumu 32.A panta 1. un 2. punkts, kurā paredzēts, ka DAS uzdevums ir uzraudzīt personas datu aizsardzības noteikumu piemērošanu, konsultēt dažādas EPO operatīvās vienības par to pienākumu izpildi un sniegt tām operatīvo dokumentāciju, kas nepieciešama datu aizsardzības prasību praktiskai īstenošanai. DAP ir jānodrošina "neatkarīga, efektīva un objektīva personas datu aizsardzībai piemērojamo noteikumu pārraudzība". Var pastāvēt cits neatkarīgs pārraudzības mehānisms, ar ko tiek pārraudzīta Apelācijas padomju atbilstība, kad tās apstrādā personas datus tiesas spriešanas funkciju ietvaros (sk. arī DAN 2. panta 6. punktu).

2.5.1. ***Neatkarība***

(80) Saskaņā ar dienesta noteikumiem DAS un DAP rīkojas pilnīgi neatkarīgi no iekšējas vai ārējas iejaukšanās to uzdevumu izpildē un pilnvaru īstenošanā ([217]). Šo principu papildina dažādi papildu aizsardzības pasākumi, kas garantē to neatkarību.

(81) DAS (un viņa vietniekus) ieceļ Priekšsēdētājs, pamatojoties uz viņu profesionālo kvalifikāciju un jo īpaši viņu speciālajām zināšanām par datu aizsardzības tiesību aktiem un praksi ([218]). DAS tiek iecelts uz atjaunojamu trīs līdz piecu gadu termiņu. Pirms tiek ierosināta DAS atbrīvošana no amata vai atlaišana, notiek apspriešanās ar DAP ([219]). Šāda iepriekšēja apspriešanās pirms DAS atbrīvošanas no amata vai atlaišanas ir paredzēta, lai nodrošinātu papildu pārbaudi un pārskatīšanu ierosinātās atbrīvošanas no amata vai atlaišanas gadījumā. Iemesli, lai ierosinātu atbrīvošanu no amata vai atlaišanu, var būt šādi ([220]): ja DAS vairs neatbilst savu pienākumu izpildei nepieciešamajiem nosacījumiem ([221]); profesionālas nekompetences dēļ ([222]); disciplināru pasākumu piemērošanas rezultātā ([223]). DAN arī nosaka, ka DAS nevar atlaist vai sodīt par tā uzdevumu izpildi, un viņš nevar pieņemt nekādus norādījumus ([224]). DAS ir jāiesaista visos personas datu aizsardzības jautājumos, un viņš katru gadu sagatavo darbības pārskatus Priekšsēdētājam un Administratīvajai padomei ([225]). Iestādei ir jānodrošina DAS viņa uzdevumu veikšanai nepieciešamie resursi ([226]).

(82) DAP sastāvā ir trīs ārējie eksperti datu aizsardzības jomā, proti, priekšsēdētājs un divi citi locekļi ([227]), kā arī locekļa aizstājējs, ko uz atjaunojamu trīs gadu termiņu ieceļ EPO Priekšsēdētājs ([228]). DAP locekļiem ir jābūt kvalifikācijai, kas vajadzīga iecelšanai tiesneša amatā, vai jābūt datu aizsardzības speciālistiem ar apliecinātām zināšanām un pieredzi datu aizsardzības tiesību jomā, kas iegūta valsts vai starptautiskā līmenī. Viņi nedrīkst būt ne EPO darbinieki, ne būt bijuši tur nodarbināti pēdējo desmit gadu laikā ([229]). Saskaņā ar DAN 48. panta 6. punktu DAP locekļi, pildot savas funkcijas, ir pilnīgi neatkarīgi. Jo īpaši DAP locekļi nedrīkst lūgt norādījumus Iestādei vai Administratīvajai padomei, un tiem nevar būt saistoši šādi norādījumi. DAP reglamentā ir arī paredzēts, ka, pildot savus uzdevumus, tai ir jārīkojas objektīvi un pilnīgi neatkarīgi ([230]). Turklāt EPO var atbrīvot DAP locekļus no viņu pienākumu pildīšanas tikai nopietnu iemeslu dēļ ([231]). DAP locekļiem ir saistošs konfidencialitātes pienākums ([232]), un viņi nedrīkst skatīt

([217]) Dienesta noteikumu 32.A panta 4. un 5. punkts.
([218]) DAN 41. pants.
([219]) DAN 42. panta 8. punkts. Šī apspriešana notiek neatkarīgi no ierosinātās atbrīvošanas no amata vai atlaišanas pamata vai iemesla.
([220]) Dienesta noteikumu 50. pants.
([221]) Sk. dienesta noteikumu 53. panta 1. punktu, kurā noteikts, ka "[i]ecēlējinstitūcija var nolemt izbeigt ar darbinieku dienesta attiecības: a) ja līgumslēdzēja valsts, kuras pilsonis ir darbinieks, pārstāj būt konvencijas līgumslēdzēja puse; b) ja darbinieks atsakās tikt pārcelts uz valsti, kas nav valsts, kurā viņš strādā; c) ja attiecībā uz darbinieku, ko Administratīvā padome iecēlusi saskaņā ar konvencijas 11. panta 1. un 2. punktu, Administratīvā padome tā nolemj organizācijas interesēs; d) ja darbinieks ir nepārtraukti nostrādājis vienu gadu vai mazāk amatā, kur iecelts uz noteiktu laiku; e) ja paša rīcības dēļ viņš vairs neatbilst 8. panta a) vai b) punktā paredzētajiem nosacījumiem [proti, viņš ir kādas EPO līgumslēdzējas valsts pilsonis, ja vien iecēlējinstitūcija nav atļāvusi izņēmumu, un viņam ir visas pilsoņa tiesības]; f) citos gadījumos, kas skaidri paredzēti šajos dienesta noteikumos".
Sk. arī dienesta noteikumu 13. panta 4. punkta b) apakšpunktu, kurā noteikts, ka "ziņojumu par pārbaudāmo var sagatavot jebkurā pārbaudes laika brīdī, ja viņa pienākumu izpilde, efektivitāte un uzvedība ir nepieņemama. Pamatojoties uz pārbaudes laika ziņojumu vai ziņojumiem, iecēlējinstitūcija var:
- atlaist jaunu darbinieku, kurš iziet pārbaudes laiku;
- nolemt, ka pārbaudāmais, kurš ir pārcelts, paaugstināts vai pārcelts citā amatā, atgriežas vai nu iepriekšējā amatā, vai, ja tas ir aizpildīts, amatā, kas atbilst viņa iepriekšējā amata pakāpei, kura prasībām viņš atbilst".
([222]) Dienesta noteikumu 52. pantā ir paredzēti kritēriji un procesi, kas jāievēro identificētas "profesionālās nekompetences" gadījumā.
([223]) Dienesta noteikumu 94. pants.
([224]) DAN 42. panta 3. punkts. Lai gan DAS var pildīt arī citus uzdevumus, šie uzdevumi nedrīkst radīt interešu konfliktu (DAN 42. panta 6. punkts).
([225]) DAN 42. panta 1. un 3. punkts.
([226]) DAN 42. panta 2. punkts.
([227]) DAN 48. panta 1. punkts.
([228]) DAN 48. panta 1. un 3. punkts.
([229]) DAN 48. panta 2. punkts.
([230]) Datu aizsardzības padomes reglamenta 1. panta 1. punkts, CA/26/21 Add. 1, pieņemts 2021. gada 11. jūnijā. Pieejams tīmekļa vietnē https://link.epo.org/web/data_protection_board-rules_of_procedure_en.pdf.
([231]) Konkrēti, līgumā ir paredzēts, ka [DAP loceklis] to "var izbeigt, neskarot tiesības izbeigt līgumu nopietnu iemeslu dēļ, [tikai] sešus (6) mēnešus iepriekš rakstveidā paziņojot par to". Tā kā dienesta līgumu reglamentē Vācijas tiesības, jēdziens "nopietns iemesls" ir jāinterpretē saskaņā ar Vācijas Civilkodeksa 626. pantu. Saskaņā ar judikatūru tas var notikt, piemēram, gadījumā, ja atkārtoti un nemainīgi tiek pārkāpti darba pienākumi (piemēram, attiecībā uz interešu konfliktu) vai ja persona nonāk ieslodzījumā.
([232]) DAN 48. panta 5. punkts.

lietas, kurās viņiem ir interešu konflikts, it īpaši personiska interese ([233]). EPO ir jāatbalsta DAP tās uzdevumu izpildē, piešķirot tai nepieciešamos resursus, kā arī juridisko un administratīvo atbalstu (ar sekretariāta starpniecību un nodrošinot DAP piekļuvi personas datiem un apstrādes darbībām) ([234]).

2.5.2. ***Uzdevumi un pilnvaras***

(83) DAS uzdevumi tostarp ir šādi: informēt pārzini vai apstrādātājus par viņu pienākumiem un attiecīgi tos konsultēt; palielināt apstrādes darbībās iesaistītā personāla informētību un nodrošināt apmācību; nodrošināt, ka datu subjekti tiek informēti par viņu tiesībām saskaņā ar DAN; neatkarīgā veidā uzraudzīt DAN, kā arī citu EPO tiesību normu, kas ietekmē datu aizsardzību, iekšējo piemērošanu un ievērošanu ([235]). Datu subjekti var sazināties ar DAS par jebkuru jautājumu, kas saistīts ar viņu datu apstrādi vai viņu tiesību īstenošanu ([236]), un pārzinis un apstrādātāji var apspriesties ar DAS par jebkuru jautājumu, kas attiecas uz DAN interpretāciju un piemērošanu ([237]).

(84) Pildot savu pārraudzības funkciju, DAS ir pilnvaras veikt datu aizsardzības revīzijas un izmeklēšanas ([238]). Revīzijas uzsāk DAS saskaņā ar gada revīzijas plānu, kas sagatavots, konsultējoties ar DAP ([239]). Revīzijā galvenā uzmanība tiek pievērsta datu aizsardzības ierakstu, paziņojumu un attiecīgās dokumentācijas novērtēšanai, piemēram, lai pārbaudītu attiecīgās datu aizsardzības dokumentācijas precizitāti un pilnīgumu, riska pārvaldības metodikas pareizu piemērošanu, datu subjektiem sniegto atbilžu precizitāti un savlaicīgumu vai attiecīga skaita datu aizsardzības ietekmes novērtējumu pienācīgu veikšanu ([240]). Saskaņā ar informāciju, ko Komisija ir saņēmusi no DAS, 2023. gadā tika veiktas trīs revīzijas un 2024. gadā – četras. Izmeklēšanu var sākt DAS pēc savas iniciatīvas, pamatojoties uz pieprasījumu, kas saņemts no DAP vai EPO struktūras (piemēram, Priekšsēdētāja vai deleģēta pārziņa), vai pamatojoties uz informāciju, kas saņemta citā ceļā (tai skaitā, piemēram, no trešām personām un fiziskām personām) ([241]). DAP pieprasītās izmeklēšanas DAS veic neatkarīgi. DAP var sniegt piezīmes un/vai pieprasīt papildu izmeklēšanu par jebkuru jautājumu, kas varētu rasties ([242]). Pārbaudes ir vērstas uz apstrādes darbībām vai konkrētiem to aspektiem vai ar tām saistītiem atgadījumiem, lai nodrošinātu, ka attiecīgā apstrāde atbilst DAN prasībām, un lai nodrošinātu datu subjektu tiesību un brīvību aizsardzību ([243]).

(85) DAS ir piekļuve visai attiecīgajai informācijai, tostarp apstrādātajiem personas datiem, kā arī visiem birojiem, datu apstrādes iekārtām un datu nesējiem ([244]). Visiem EPO darbiniekiem un operatīvajām nodaļām ir jāpalīdz DAS veikt tā pienākumus, tostarp nodrošinot piekļuvi telpām un attiecīgajai informācijai ([245]).

([233]) DAN 48. panta 7. punkts.
([234]) DAN 48. panta 10. punkts. Sekretariāts savus uzdevumus veic neatkarīgi no nepamatotas iejaukšanās un tikai saskaņā ar DAP priekšsēdētāja norādījumiem. Tas sniedz padomei juridisku, administratīvu un loģistikas atbalstu. Sk. DAP reglamenta 2. pantu.
([235]) DAN 43. panta 1. punkts.
([236]) DAN 43. panta 1. punkta k) apakšpunkts.
([237]) DAN 42. panta 4. un 7. punkts.
([238]) DAN 43. panta 1. punkta d) apakšpunkts. Sk. arī datu aizsardzības pārraudzības dokumentu *How the Data Protection Office Conducts DP Audits and DP Inspections*, kas pieejams tīmekļa vietnē https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.
([239]) DAP var sniegt ieteikumus par jomām, kurās būtu jāveic revīzijas, sk. Datu aizsardzības pārraudzības dokumentu, 4. lpp.
([240]) Datu aizsardzības pārraudzības dokuments, 4. lpp.
([241]) Datu aizsardzības pārraudzības dokuments, 7. lpp.
([242]) Datu aizsardzības pārraudzības dokuments, 6. lpp.
([243]) Datu aizsardzības pārraudzības dokuments, 6. lpp.
([244]) DAN 43. panta 5. punkts.
([245]) DAN 46. pants.

(86) Kad revīzija vai izmeklēšana ir pabeigta, DAS pieņem ziņojumu, kurā izklāsta savus konstatējumus, secinājumus un ieteiktos korektīvos pasākumus ([246]). Šādi pasākumi var ietvert, piemēram, preventīvus vai sekas mazinošus pasākumus atbilstības uzlabošanai, kā arī pasākumus neatbilstības novēršanai (piemēram, lai panāktu apstrādes atbilstību DAN, apstrādātu datu subjektu pieprasījumus īstenot savas tiesības, apturētu vai izbeigtu apstrādi utt.) ([247]). DAS var arī informēt kompetento iecēlējinstitūciju par to, ka darbinieki neievēro DAN, un ieteikt sākt administratīvu izmeklēšanu, lai noteiktu, vai ir vajadzīgas disciplināras vai cita veida darbības ([248]). Saskaņā ar dienesta noteikumiem ikvienam darbiniekam, kas tīši vai nolaidības dēļ neievēro DAN, var piemērot disciplinārsodu vai citu pasākumu ([249]).

(87) Revīziju un izmeklēšanas rezultāti ir jāpaziņo DAP ([250]). Revīzijas vai izmeklēšanas ziņojums pēc pieprasījuma ir jāiesniedz DAP. DAP ir atļauts komentēt DAS ziņojumu, tostarp par DAS konstatējumiem attiecībā uz to, vai ir noticis DAN pārkāpums, par ierosinātajiem korektīvajiem pasākumiem, un tā var pieprasīt papildu izmeklēšanas pasākumus ([251]). Ja DAS veiktā revīzijā vai pārbaudē tiek secināts, ka ir pieļauta neatbilstība (t. i., DAN pārkāpums), DAS ziņojums ir jāiesniedz DAP secinājumu un ieteikto korektīvo pasākumu apstiprināšanai. Ja DAP nepiekrīt DAS secinājumiem vai ieteiktajiem korektīvajiem pasākumiem, DAP savus komentārus, tostarp nolūkā grozīt ierosinātos secinājumus un ieteiktos korektīvos pasākumus, dara zināmus DAS, kam tie būtu attiecīgi jāīsteno. DAP apstiprinātie korektīvie pasākumi ir saistoši pārzinim un deleģētajiem pārziņiem, un fiziskas personas uz tiem var atsaukties, pirms tiek izmantoti 95. apsvērumā aprakstītie tiesiskās aizsardzības mehānismi ([252]). DAS ir jāpārbauda korektīvo pasākumu īstenošana (principā sešus mēnešus pēc to paziņošanas) un katru gadu jāziņo Priekšsēdētājam par īstenošanas stāvokli ([253]).

(88) DAP uzdevums ir ne tikai nodrošināt DAN ievērošanu, bet arī konsultēt Priekšsēdētāju par lēmumu par aizsardzības līmeņa pietiekamību pieņemšanu, konsultēt pārzini par nepieciešamību veikt novērtējumu par ietekmi uz datu aizsardzību un izskatīt fizisku personu sūdzības (sk. 92.–96. apsvērumu) ([254]).

2.6. **Tiesiskā aizsardzība**

(89) Lai nodrošinātu pietiekamu aizsardzību un jo īpaši individuālo tiesību īstenošanu, datu subjektam vajadzētu būt pieejamiem efektīviem tiesiskās aizsardzības līdzekļiem, tostarp kompensācijai par kaitējumu.

(90) EPO tiesiskais regulējums piedāvā privātpersonām vairākas dažādas tiesiskās aizsardzības iespējas.

(91) Pirmkārt, datu subjekti, kuri uzskata, ka EPO veiktā personas datu apstrāde pārkāpj viņu tiesības (t. i., pārkāpj DAN), var pieprasīt pārskatīšanu, ko veic deleģētais pārzinis saskaņā ar DAN 49. pantu. Deleģētais pārzinis izskatīs sūdzību un pieņems lēmumu ([255]). Pirms lēmuma pieņemšanas deleģētajam pārzinim ir jāapspriežas ar DAS, kas sniedz rakstisku atzinumu ne vēlāk kā piecpadsmit kalendārās dienas pēc pārskatīšanas pieprasījuma saņemšanas ([256]). Deleģētajam pārzinim ir jāatbild personai viena mēneša laikā no pieprasījuma saņemšanas dienas ([257]). Lēmums jāpaziņo personai kopā ar informāciju par tālākām pārsūdzības iespējām ([258]). Ja deleģētais pārzinis neveic nekādas

([246]) Datu aizsardzības pārraudzības dokuments.
([247]) Datu aizsardzības pārraudzības dokuments, 2. lpp. ("ieteikumu" definīcija).
([248]) DAN 43. panta 6. punkts.
([249]) DAN 54. pants. Disciplinārsodus piemēro Priekšsēdētājs, kuram ir disciplināras pilnvaras un tiesības veikt disciplinārus pasākumus attiecībā uz EPO personālu, sk. EPK 10. pantu un dienesta noteikumu 93. pantu un turpmākos pantus.
([250]) Datu aizsardzības pārraudzības dokuments, 7. lpp.
([251]) Datu aizsardzības pārraudzības dokuments, 3.–4. un 8. lpp.
([252]) Eiropas Patentu iestādes Priekšsēdētāja 2024. gada 12. jūlija lēmums par Datu aizsardzības padomes apstiprināto DAS ieteikumu izpildāmību saistībā ar datu aizsardzības revīzijām un inspekcijām, https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf.
([253]) Datu aizsardzības pārraudzības dokuments, 5. un 9. lpp.
([254]) DAN 47. pants.
([255]) DAN 49. panta 1. punkts. Pieprasījums jāiesniedz ne vēlāk kā trīs mēnešus no dienas, kad datu subjekts ticis informēts vai citādi uzzinājis par tādu personas datu apstrādi, ar kuru, iespējams, tiek pārkāptas viņa tiesības.
([256]) DAN 49. panta 2. punkts. Ja DAS nesniedz atzinumu līdz šā perioda beigām, atzinums vairs nav vajadzīgs.
([257]) DAN 49. panta 3. punkts. Vajadzības gadījumā minēto termiņu var pagarināt vēl par diviem mēnešiem, ņemot vērā pieprasījumu sarežģītību un skaitu. Termiņa pagarināšanas gadījumā deleģētajam pārzinim par to un par kavēšanās iemesliem jāpaziņo datu subjektam viena mēneša laikā pēc pārskatīšanas pieprasījuma saņemšanas.
([258]) DAN 49. panta 3. punkts.

darbības trīs mēnešu laikā, to uzskata par pieprasījuma netiešu noraidīšanu.

(92) Otrkārt, privātpersonas var apstrīdēt deleģētā pārziņa lēmumu vai pārskatīšanas pieprasījuma netiešu noraidīšanu, iesniedzot sūdzību DAP ([259]).

(93) Izskatot sūdzību, DAP ir jāaicina datu subjekts, pārzinis un attiecīgā gadījumā apstrādātājs rakstiski izklāstīt savu nostāju par strīdīgajiem apgalvojumiem un faktiem un sniegt pierādījumus vai komentārus un argumentus par pieejamajiem pierādījumiem ([260]). Šajā kontekstā DAP var pieprasīt no pusēm jebkādu informāciju, kas tai vajadzīga sūdzības izskatīšanai, un papildus var iegūt papildu informāciju ar DAS starpniecību ([261]). Lemjot par nepieciešamo turpmāko rīcību saistībā ar sūdzību, DAP tostarp ir jāņem vērā iespējamā pārkāpuma raksturs un smagums, skarto datu subjektu skaits, ietekmēto datu kategorijas un pārkāpuma ilgums ([262]). DAP var aicināt puses panākt izlīgumu, mudina uz šādu izlīgumu un aktīvi veicina tā panākšanu ([263]). Sūdzības iesniedzējs var arī lūgt DAP piemērot steidzamības procedūru iespējamā pārkāpuma smaguma vai personu tiesībām radītā riska nopietnības dēļ ([264]).

(94) Pēc sūdzības izskatīšanas DAP sniedz pārzinim argumentētu atzinumu, kurā ietver faktu izklāstu, pušu galvenos argumentus, DAP apsvērumus un ieteikumus ([265]). Steidzamības procedūras gadījumā DAP divu mēnešu laikā pēc sūdzības iesniegšanas ir oficiāli jāsniedz argumentēts atzinums ([266]). Savā argumentētajā atzinumā DAP var sniegt jebkādus ieteikumus, ko tā uzskata par nepieciešamiem, tostarp pienākumrīkojumus (piemēram, izbeigt nelikumīgu datu apstrādi, dzēst nelikumīgi apstrādātus datus), materiālā vai nemateriālā kaitējuma atlīdzināšanu ([267]). Pamatotais atzinums ir jāpaziņo datu subjektam un pārzinim (t. i., Iestādes Priekšsēdētājam, Apelācijas padomju priekšsēdētājam, Administratīvās padomes priekšsēdētājam vai izraudzītās komitejas priekšsēdētājam atkarībā no tā, vai sūdzība attiecas uz Iestādi, Apelācijas padomēm, padomi vai izraudzīto komiteju). Pēc tam pārzinis pieņems galīgo saistošo lēmumu pēc DAP argumentētā atzinuma ([268]). Galīgo lēmumu paziņo datu subjektam, DAP un DAS ([269]). Ja pārzinis izlemj neievērot vienu vai vairākus argumentētā atzinuma aspektus, tas to rakstiski paskaidro lēmumā ([270]).

(95) Datu subjekts, kurš nav apmierināts ar pārziņa lēmumu, var to pārsūdzēt tālāk, atsaucoties uz DAP argumentēto atzinumu. EPO darbinieki var apstrīdēt lēmumu Starptautiskās Darba organizācijas Administratīvajā tiesā ([271]). Jebkurš cits datu subjekts, kas nepiekrīt pārziņa lēmumam, trīs mēnešu laikā pēc lēmuma saņemšanas var iesniegt Priekšsēdētājam pieprasījumu par *ad hoc* šķīrējtiesu ([272]). DAP ir paredzēta īpaša procedūra, kas jāievēro *ad hoc* šķīrējtiesas gadījumā ([273]). Konkrēti, trīs mēnešu laikā pēc datu subjekta pieprasījuma saņemšanas Pastāvīgās

([259]) DAN 50. panta 1. punkts. Sūdzība DAP ir jāiesniedz trīs mēnešu laikā pēc lēmuma saņemšanas vai netieša noraidījuma gadījumā – no dienas, kad beidzies termiņš atbildes sniegšanai uz pieprasījumu.
([260]) DAN 50. panta 2. punkts.
([261]) Respektīvi, DAS ir pienākums atbildēt uz DAP pieprasījumiem un sadarboties ar to (DAN 43. panta i) punkts). DAS ir arī jāveicina sadarbība starp DAP un Iestādi, un šajā kontekstā tam ir piekļuve jebkurai būtiskai informācijai (DAN 43. panta j) punkts, 46. panta a) un b) punkts).
([262]) DAP reglamenta 4. panta 5. punkts.
([263]) DAP reglamenta 8. pants.
([264]) DAP reglamenta 11. panta 1. punkts.
([265]) DAP reglamenta 10. panta 2. punkts.
([266]) DAP reglamenta 11. panta 2. punkts.
([267]) DAN 50. panta 3. punkts.
([268]) DAN 50. panta 4. punkts un DAP 10. panta 6. punkts.
([269]) DAN 50. panta 6. punkts.
([270]) DAN 50. panta 4. punkts. Ja DAP ieteikumi nav tieši attiecināmi uz datu subjektiem, pārzinis iespējamās atkāpes izklāsta rakstiski dokumentā, ko iesniedz DAP.
([271]) DAN 50. panta 7. punkts. Sk. EPK 13. pantu un dienesta noteikumu 113. pantu.
([272]) DAN 50. panta 8. punkts un 52. panta 2. punkts. Saskaņā ar Administratīvās padomes DAN un izvēlētās komitejas DAN šķīrējtiesu var pieprasīt Administratīvās padomes priekšsēdētājam.
([273]) DAN 52. panta 1. punkts.

šķīrējtiesas ģenerālsekretāram ir jāieceļ viens šķīrējtiesnesis, pamatojoties uz DAN noteiktajiem kritērijiem ([274]). Šķīrējtiesnesim jābūt juridiski kvalificētam, ar atļauju praktizēt jurisprudenci vienā no EPO līgumslēdzējām valstīm, jāspēj pierādīt attiecīgas speciālās zināšanas datu aizsardzības jautājumos un jāpārzina tiesību akti, kas reglamentē starptautiskās organizācijas ([275]). Papildus šo kritēriju izpildei var iecelt tikai personas, kas nav strādājušas ne EPO, ne datu subjekta labā vai dienestā. DAN ir paredzēts, ka šķīrējtiesnesim ir jārīkojas neatkarīgi un objektīvi ([276]), jāizturas vienlīdzīgi pret abām pusēm un jādod tām iespēja izklāstīt savu nostāju katrā procesa posmā ([277]). Šķīrējtiesas procesi nav publiski ([278]), un tos reglamentē EPK, DAN, tostarp jebkuri īstenošanas tiesību akti, starptautisko organizāciju tiesības un starptautisko publisko tiesību principi ([279]). Lai gan katra puse sedz savas izmaksas un juridiskās pārstāvības izdevumus (ja vien šķīrējtiesnesis nenolemj citādi), šķīrējtiesneša honorārus un izdevumus, iespējamo ekspertu konsultāciju un liecinieku izmaksas sedz EPO ([280]). Izlīgums ir jānoslēdz rakstiska šķīrējtiesas nolēmuma formā, par kuru panākta vienošanās un kurš ir galīgs un saistošs ([281]).

(96) Jebkura persona, kurai nodarīts kaitējums DAN pārkāpuma dēļ, var pieprasīt no EPO kompensāciju, izmantojot 91.–95. apsvērumā aprakstītās procedūras ([282]). EPO netiek saukta pie atbildības, ja tā pierāda, ka nav atbildīga par kaitējumu izraisījušo notikumu.

3. PUBLISKU IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO EIROPAS PATENTU BIROJAM NOSŪTA NO SAVIENĪBAS, UN TO IZMANTOŠANA

(97) Tiesiskais regulējums, saskaņā ar kuru EPO novērtē publisko iestāžu – līgumslēdzēju valstu un trešo valstu – pieprasījumus attiecībā uz personas datiem, ko apstrādā EPO, un atbild uz tiem, izriet no EPO Protokola par privilēģijām un imunitāti (PPI) ([283]), DAN prasībām par personas datu nosūtīšanu un pārsūtīšanu un starptautiskajām publiskajām tiesībām.

(98) Pirmkārt, uz personas datu apstrādi, ko EPO veic savu oficiālo darbību nolūkā, attiecas organizācijas imunitāte. EPO imunitāti papildina sadarbības pienākums, kas noteikts PPI 20. pantā. Līdz ar to ikvienu līgumslēdzējas valsts iestādes lūgumu iegūt EPO apstrādātos datus izvērtē Priekšsēdētājs saskaņā ar PPI 20. panta 1. punktu, kurā noteikts, ka organizācija "vienmēr sadarbojas ar līgumslēdzēju valstu kompetentajām iestādēm, lai veicinātu pareizu tiesvedību, nodrošinātu policijas, sabiedrības veselības, darba inspekcijas vai citu līdzīgu valsts tiesību aktu ievērošanu un novērstu jebkādu šajā protokolā paredzēto privilēģiju, imunitātes un iespēju ļaunprātīgu izmantošanu". Izņēmuma kārtā organizācija var atcelt savu imunitāti pret tiesvedību un izpildi ([284]). Lemjot par sadarbības pieprasījumu, Priekšsēdētājam ir rīcības brīvība, apsverot lūguma atbilstību organizācijas tiesiskajam regulējumam ([285]). Secinājums var būt tāds, ka Iestāde var atbildēt uz PPI pieprasījumu un izpaust personas datus tikai saskaņā ar DAN noteiktajām datu nosūtīšanas prasībām (sk. 62.–67. apsvērumu). Saskaņā ar DAN saņēmējam ir jāsniedz pierādījumi, ka dati ir jānosūta konkrētam mērķim, kas izriet no EPO saistībām sadarboties ar līgumslēdzēju valsti vai valstīm ([286]). Pārzinim attiecībā uz katru nosūtīšanu jāspēj pierādīt, ka šāda nosūtīšana ir nepieciešama un samērīga ar konkrēto nolūku, kādā tā tiek veikta ([287]). Datu pārsūtīšanai jānotiek tā, lai nodrošinātu, ka tiek saglabāts DAN noteiktais aizsardzības līmenis ([288]). Saskaņā ar DAS sniegtajiem norādījumiem tas nozīmē, ka tiek nodrošināti atbilstoši aizsardzības pasākumi, tai skaitā kopīgojamie dati ir jāsamazina līdz minimumam un jāaprobežojas ar to, kas ir

([274]) DAN 52. panta 4. punkts.
([275]) DAN 52. panta 4. punkts.
([276]) DAN 52. panta 4. punkts.
([277]) DAN 52. panta 8. punkts.
([278]) DAN 52. panta 9. punkts.
([279]) DAN 52. panta 6. punkts. Šķīrējtiesas vieta ir Hāga (DAN 52. panta 5. punkts), un tiesvedības laikā izmantotā valoda ir jāizvēlas šķīrējtiesnesim, kas tomēr ir viena no EPO oficiālajām valodām (angļu, franču vai vācu valoda) (DAN 52. panta 7. punkts).
([280]) DAN 52. panta 13. punkts.
([281]) DAN 52. panta 10. punkts. Sk. arī Pastāvīgās šķīrējtiesas reglamenta 3. pantu un 34. panta 2. punktu.
([282]) DAN 53. pants. Saskaņā ar EPK 9. panta 2. punktu noteiktos apstākļos (jo īpaši saskaņā ar Vācijas tiesību aktos piemērojamām prasībām) privātpersonas var saņemt arī kompensāciju par kaitējumu, ko radījis EPO personāls, pildot savus pienākumus.
([283]) EPO protokols par privilēģijām un imunitāti. Pieejams tīmekļa vietnē https://www.epo.org/en/legal/epc/2020/proprim.html.
([284]) PPI 3. panta 1. punkta a) apakšpunkts.
([285]) Ietverot iespēju pieprasījumu noraidīt.
([286]) DAN 8. panta 3. punkts.
([287]) DAN 8. panta 4. punkts.
([288]) Paskaidrojošais dokuments "EPO personas datu nosūtīšana un pārsūtīšana" (nosūtīšanas un pārsūtīšanas dokuments), pieejams tīmekļa vietnē https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, 4. lpp. Konkrēti, sk. "EPO DAN [...] nosaka vispārēju pienācīgas aizsardzības principu, kas jo īpaši piemērojams starptautiskai datu plūsmai".

pienācīgs, atbilstošs un absolūti nepieciešams šā mērķa sasniegšanai ([289]). Ja ir pamats uzskatīt, ka var tikt skartas attiecīgās personas tiesības un brīvības, pārzinim pēc dažādo interešu izsvēršanas ir jāpierāda, ka personas datu nosūtīšana šim konkrētajam nolūkam ir samērīga ([290]).

(99) Otrkārt, EPO nav piemērojams neviens juridisks instruments, kas konkrēti reglamentētu trešo valstu (t. i., valstu, kas nav EPO līgumslēdzēja puse) iestāžu pieprasījumus saņemt EPO apstrādātos datus. Tādējādi jebkāda izpaušana, atbildot uz šādu pieprasījumu, var notikt tikai tad, ja ir izpildītas DAN noteiktās prasības par starptautisku datu pārsūtīšanu (kā aprakstīts 68.–73. apsvērumā). Tas tā ir tikai tad, ja par attiecīgo valsti ir pieņemts lēmums par aizsardzības līmeņa pietiekamību, kas attiecas uz nosūtīšanu, ja ir ieviesti atbilstoši aizsardzības pasākumi vai ja tiek piemērota atkāpe.

(100) To, kā Priekšsēdētājs ievēro PPI, ieskaitot veidu, kā tiek reaģēts uz publisko iestāžu sadarbības pieprasījumiem, uzrauga Administratīvā padome, savukārt DAN noteikto personas datu nosūtīšanas un pārsūtīšanas prasību ievērošana ir pakļauta DAS un DAP uzraudzībai, kā aprakstīts 84.–88. apsvērumā. Privātpersonas var izmantot 90.–96. apsvērumā aprakstītos tiesiskās aizsardzības līdzekļus attiecībā uz savu personas datu nosūtīšanu vai pārsūtīšanu, ja tā notikusi, pārkāpjot DAN.

4. SECINĀJUMI

(101) Komisija uzskata, ka EPO no Savienības nosūtītajiem personas datiem nodrošina aizsardzības līmeni, kas būtībā ir līdzvērtīgs Regulā (ES) 2016/679 garantētajam aizsardzības līmenim.

(102) Ņemot vērā šā lēmuma konstatējumus, būtu jālemj, ka EPO nodrošina pietiekamu aizsardzības līmeni Regulas (ES) 2016/679 45. panta nozīmē, interpretējot to saskaņā ar Eiropas Savienības Pamattiesību hartu, attiecībā uz personas datiem, kas no Savienības tiek nosūtīti EPO.

5. ŠĀ LĒMUMA SEKAS UN DATU AIZSARDZĪBAS IESTĀŽU RĪCĪBA

(103) Dalībvalstīm un to struktūrām ir pienākums veikt nepieciešamos pasākumus, lai izpildītu Savienības iestāžu tiesību aktus, jo tie tiek uzskatīti par likumīgiem un attiecīgi paredz tiesiskās sekas līdz brīdim, kad tiek atcelti, anulēti saskaņā ar prasību atcelt tiesību aktu vai pasludināti par spēkā neesošiem pēc lūguma sniegt prejudiciālu nolēmumu vai iebildes par nelikumību.

(104) Tādējādi lēmums par aizsardzības līmeņa pietiekamību, ko Komisija pieņēmusi saskaņā ar Regulas (ES) 2016/679 45. panta 3. punktu, ir saistošs visām dalībvalstu struktūrām, kurām tas adresēts, arī to neatkarīgajām uzraudzības iestādēm. Konkrētāk, pārzinis vai apstrādātājs Savienībā var nosūtīt datus EPO bez jebkādas turpmākas atļaujas saņemšanas.

([289]) Nosūtīšanas un pārsūtīšanas dokuments, 12. zemsvītras piezīme.
([290]) DAN 8. panta 3. punkts.

(105) Vienlaikus būtu jāatgādina, ka saskaņā ar Regulas (ES) 2016/679 58. panta 5. punktu un kā Tiesa paskaidrojusi lietā C-362/14 ([291]), ja valsts datu aizsardzības iestāde, arī pēc sūdzības saņemšanas, apšauba Komisijas lēmuma par aizsardzības līmeņa pietiekamību atbilstību fiziskas personas pamattiesībām uz privātumu un datu aizsardzību, tai valsts tiesību aktos ir jānodrošina tiesiskās aizsardzības līdzeklis, kas ļauj celt šādus iebildumus valsts tiesā, kurai var būt pienākums lūgt Tiesai sniegt prejudiciālu nolēmumu.

6. ŠĀ LĒMUMA UZRAUDZĪBA, APTURĒŠANA, ATCELŠANA VAI GROZĪŠANA

(106) Saskaņā ar Eiropas Savienības Tiesas judikatūru un atbilstoši Regulas (ES) 2016/679 45. panta 4. punktam Komisijai pēc lēmuma par aizsardzības līmeņa pietiekamību pieņemšanas būtu pastāvīgi jāuzrauga norises attiecīgajā trešā valstī vai starptautiskajā organizācijā, lai novērtētu, vai tā joprojām nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni. Vajadzība pēc šāda vērtējuma katrā ziņā rodas, ja Komisija saņem informāciju, kura rada šaubas par to.

(107) Tāpēc Komisijai būtu pastāvīgi jāuzrauga situācija ar EPO personas datu apstrādes tiesisko regulējumu un faktisko praksi, kas novērtēta šajā lēmumā. Lai atvieglotu šo procesu, EPO tiek aicināta informēt Komisiju par būtiskām ar šo lēmumu saistītām norisēm – gan attiecībā uz personas datu apstrādi, gan ierobežojumiem un garantijām, kas piemērojami, kad publiskās iestādes piekļūst personas datiem.

(108) Turklāt, lai Komisija varētu efektīvi pildīt savu uzraudzības funkciju, dalībvalstīm būtu jāinformē Komisija par visām būtiskajām darbībām, ko veikušas valstu datu aizsardzības iestādes, jo īpaši attiecībā uz Savienības datu subjektu vaicājumiem un sūdzībām par personas datu nosūtīšanu no Savienības uz EPO.

(109) Piemērojot Regulas (ES) 2016/679 45. panta 3. punktu un ņemot vērā faktu, ka ar EPO tiesisko regulējumu nodrošinātais aizsardzības līmenis var mainīties, Komisijai pēc šā lēmuma pieņemšanas būtu periodiski jāpārbauda, vai konstatējumi par EPO nodrošinātā aizsardzības līmeņa pietiekamību joprojām ir faktiski un juridiski pamatoti. Šādai izvērtēšanai būtu jānotiek vismaz reizi četros gados, un tai būtu jāaptver visi šā lēmuma darbības aspekti, tostarp attiecīgo pārraudzības un izpildes mehānismu darbība.

(110) Lai veiktu šo pārskatīšanu, Komisijai būtu jātiekas ar EPO, tostarp tās DAS un DAP. Būtu jānodrošina iespēja arī Eiropas Datu aizsardzības kolēģijas pārstāvjiem apmeklēt šādas sanāksmes. Pārskatīšanas ietvaros Komisijai būtu jāprasa, lai EPO sniedz vispusīgu informāciju par visiem aspektiem, kas ir būtiski konstatējumam par aizsardzības līmeņa pietiekamību. Komisijai arī būtu jāprasa paskaidrojumi par jebkuru informāciju, kas ir būtiska šim lēmumam un ko tā saņēmusi no Eiropas Datu aizsardzības kolēģijas, individuālām datu aizsardzības iestādēm, pilsoniskās sabiedrības grupām, publiskiem vai plašsaziņas līdzekļu ziņojumiem vai jebkuriem citiem pieejamiem informācijas avotiem.

(111) Pamatojoties uz pārskatīšanu, Komisijai būtu jāsagatavo publisks ziņojums, kas jāiesniedz Eiropas Parlamentam un Padomei.

(112) Ja pieejamā informācija, sevišķi informācija, kas izriet no tā, ka Komisija uzrauga norises, kuras varētu ietekmēt šā lēmuma darbību saskaņā ar Regulas (ES) 2016/679 45. panta 4. punktu, vai ko sniegusi EPO vai dalībvalstu iestādes, liecina, ka EPO nodrošinātais aizsardzības līmenis var vairs nebūt pietiekams, Komisijai par to būtu jāinformē EPO un jāpieprasa, lai noteiktā un saprātīgā termiņā tiktu veikti atbilstoši pasākumi.

(113) Ja līdz noteiktā termiņa beigām EPO nebūs veikusi minētos pasākumus vai kā citādi apmierinoši neparādīs, ka šā lēmuma pamatā joprojām ir pietiekams aizsardzības līmenis, Komisija uzsāks Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru, lai daļēji vai pilnībā apturētu vai atceltu šo lēmumu.

([291]) Spriedums lietā C-362/14 *Schrems* ("*Schrems* I"), ECLI:EU:C:2015:650, 65. punkts.

(114) Alternatīvi Komisija uzsāks minēto procedūru, lai grozītu šo lēmumu, jo īpaši piemērojot papildu nosacījumus datu pārsūtīšanai vai ierobežojot aizsardzības līmeņa pietiekamības konstatējuma darbības jomu tikai attiecībā uz tādu datu pārsūtīšanu, kam joprojām tiek nodrošināts pietiekams aizsardzības līmenis.

(115) Komisijai būtu jāapsver šā lēmuma grozīšanas, apturēšanas vai atcelšanas procedūras sākšana arī gadījumā, ja pārskatīšanas kontekstā vai citādi EPO nesniedz informāciju vai paskaidrojumus, kas nepieciešami, lai novērtētu no Savienības uz EPO nosūtīto personas datu aizsardzības līmeni vai atbilstību šim lēmumam. Šajā saistībā Komisijai būtu jāņem vērā tas, kādā apmērā attiecīgo informāciju var iegūt no citiem avotiem.

(116) Pienācīgi pamatotu nenovēršamu steidzamu iemeslu dēļ Komisija izmantos iespēju saskaņā ar Regulas (ES) 2016/679 93. panta 3. punktā minēto procedūru pieņemt nekavējoties piemērojamus īstenošanas aktus, ar kuriem aptur, atceļ vai groza šo lēmumu.

7. NOBEIGUMA APSVĒRUMI

(117) Eiropas Datu aizsardzības kolēģija ir publiskojusi savu atzinumu ([292]), un tas tika ņemts vērā, sagatavojot šo lēmumu.

(118) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) 2016/679 93. panta 1. punktu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Regulas (ES) 2016/679 45. panta nolūkā Eiropas Patentu organizācija nodrošina pienācīgu aizsardzības līmeni personas datiem, kas no Savienības tiek nosūtīti Eiropas Patentu organizācijai.

2. pants

Lai aizsargātu personas attiecībā uz viņu personas datu apstrādi, ikreiz, kad kompetentās iestādes dalībvalstīs īsteno savas pilnvaras atbilstoši Regulas (ES) 2016/679 58. pantam attiecībā uz datu nosūtīšanu 1. pantā noteiktajā piemērošanas jomā, attiecīgā dalībvalsts nekavējoties par to informē Komisiju.

3. pants

1. Komisija pastāvīgi uzrauga, kā tiek piemērots Eiropas Patentu organizācijas tiesiskais regulējums, kas ir šā lēmuma pamatā, lai novērtētu, vai Eiropas Patentu organizācija turpina nodrošināt 1. panta nozīmē pietiekamu aizsardzības līmeni.

2. Dalībvalstis un Komisija informē viena otru par gadījumiem, kad Eiropas Patentu organizācija nespēj nodrošināt atbilstību tiesiskajam regulējumam, kas ir šā lēmuma pamatā.

3. Vismaz reizi četros gados Komisija izvērtē 1. pantā ietverto konstatējumu, pamatojoties uz visu pieejamo informāciju, tostarp informāciju, kas saņemta kopā ar Eiropas Patentu organizāciju veiktās pārskatīšanas ietvaros.

([292]) Eiropas Datu aizsardzības kolēģija, Atzinums 07/2025 par Eiropas Komisijas īstenošanas lēmuma projektu saskaņā ar Regulu (ES) 2016/679 par personas datu pienācīgu aizsardzību Eiropas Patentu organizācijā. Pieejams šeit: https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202507-epo-adequacydecision_en.pdf.

4. Ja Komisija ir konstatējusi pazīmes, ka vairs netiek nodrošināts pietiekams aizsardzības līmenis, Komisija par to informē Eiropas Patentu organizāciju. Vajadzības gadījumā Komisija var izlemt šo lēmumu apturēt, grozīt vai atcelt vai ierobežot tā piemērošanas jomu saskaņā ar Regulas (ES) 2016/679 45. panta 5. punktu.

Komisija var arī apturēt, atcelt vai grozīt šo lēmumu, ja Eiropas Patentu organizācijas nesadarbošanās neļauj Komisijai noteikt, vai ir ietekmēts šā lēmuma 1. pantā minētais novērtējums.

4. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2025. gada 15. jūlijā

Komisijas vārdā –
Komisijas loceklis
Michael MCGRATH